SUBMISSION TO THE INFORMATION AND PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

Examination of USA PATRIOT ACT implications for personal information of British Columbia residents involved in outsourcing of government services to U.S.-linked service providers

July 23, 2004

BRITISH COLUMBIA

The Province of British Columbia

105-07243/

BRITISH COLUMBIA

Ministry of Attorney General

Legal Services Branch
Constitutional & Administrative Law

MEMORANDUM

Mailing Address: PO BOX 9280 STN PROV GOVT Victoria BC V8W 9J7

Location: 1001 Douglas Street Victoria BC
Phone: 250 356-8890 Fax: 250 356-9154

July 23, 2004

David Loukidelis
Information and Privacy Commissioner
for British Columbia

Re:Exam ination of USA PATRIOT ACT implications for personal information of British Columbia residents involved in outsourcing of government services to U.S.-linked service providers – OIPC File No. 21220

Thank you for your invitation to the Government of British Columbia to make submissions regarding possible implications of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Pub.L.No. 107-56, 115 Stat. 272, (the "Patriot Act") for the personal information of British Columbians as a result of the outsourcing of government services to U.S. linked service providers. Government welcomes the opportunity to participate in this review.

Our submission focuses on the following issues you have identified for comment:

- Does the Patriot Act permit US authorities to access personal information of British Columbians that is, through the outsourcing of public services, in the custody or under the control of US linked private sector service providers? If it does, under what conditions can this occur?

- If it does, what are the implications for public body compliance with the personal privacy protections in the Freedom of Information and Protection of Privacy Act (the "FOIPP Act")? What measures can be suggested to eliminate or appropriately mitigate privacy risks affecting compliance with the FOIPP Act?

The Province has conducted a comprehensive assessment of this matter and looks forward to your report. We are committed to ensuring the necessary steps are taken to continue to ensure the protection of British Columbian's personal information.

Contents

		Found at Page
1.	Summary of Government's Position	3
2.	Existing Information Sharing and Access Mechanisms	6
	The Mutual Legal Assistance Treaty	7
	Canadian Implementation of MLA T	10
	Summary	10
	Grand Jury Subpoenas	11
	Other U.S. and Canada Law Enforcement Information Sharing Mechanisms	15
3.	Legal Framework	18
	Procedural and Physical Security Measures	20
	The Disclosure of Personal Information to Contractors	22
	Disclosure of Personal information to Comply w ith a Subpoena, Warrant or Order	24
	Sensitivity of the Personal Information	25
	Other Relevant Factors in Addressing the "Reasonable Security" Issue	26
	Service of a Patriot Act Order	32
4.	The Risk of Access to Canadian Information under the Patriot Act	35
	The Jaffer Opinion	35
	Summary	39
5.	NAFTA, WTO and AIT	41
6.	Other Security Risks	44
7.	Privacy Protection Measures	45
8.	Legislative Options	49
9.	Scope of the Patriot Act Issue	50
10.	Conclusion	52

1. SUMMARY OF GOVERNMENT'S POSITION

The Patriot Act poses only a small incremental risk. However, British Columbia is a leader in privacy protection in Canada and will take effective measures to reduce that minimal risk.

- The risk that personal information held in BC could, or would, be obtained by US authorities under the *Patriot Act* as a result of government outsourcing initiatives is small.
- To the extent that the *Patriot Act* presents only a small incremental risk to privacy, government is prepared to address that small risk by ensuring that a U.S. affiliate does not have access to, or control of, sensitive personal information provided by government to a Canadian or B.C. service provider. In addition, government will not send sensitive personal information to the US either on a temporary or permanent basis.
- Government will consult with stakeholders, including your office, and develop legislative amendments to build on what is already the strongest privacy legislation in Canada. The proposed amendments will expressly prohibit service providers from disclosing personal information that has been provided to them by public bodies unless permitted by the FOIPP Act, and require that such service providers notify government in the event their foreign affiliate requests that they disclose such information.

Government recognizes and takes seriously its obligation and commitment to protect the personal information of British Columbians.

- British Columbia has strong privacy legislation. We are regarded as national leaders in privacy protection. We take that leadership role, and our obligation to protect privacy, seriously.
- The Province sought and obtained U.S. advice to deal with concerns about the *Patriot Act*. The Province has carefully considered those concerns.

The privacy issues raised by the Patriot Act are only a small part of the constant concern that governments and private bodies and individuals will always have about balancing the need for security and law enforcement in an interconnected global economy with respect for privacy.

- The issues raised by the *Patriot Act* are not unique to government or to Alternative Service Delivery (ASD) initiatives. They apply to personal

information held by the private sector, not just to personal information held by public bodies. As such, the present issues under review are not just issues for government. They are also issues for the private sector.

The benefits of Government's innovative approach to service delivery, including improved service to British Columbians, must not be lost in a climate of unfounded fear about loss of privacy under the Patriot Act.

- As you have recently recognized in dealing with issues relating to security, we must deal with real risk, and not pander to fear. When one considers the real risk of access under the *Patriot Act* dispassionately, one recognizes that that it is only a small incremental risk. This is fully explained below.
- ASD initiatives will result in more effective programs and better service delivery to the public. The Province will continue with these initiatives to ensure that the public receives these benefits. Although there is only a small incremental risk associated with the *Patriot Act* and ASD initiatives, government will continue to develop public policy that benefits British Columbians and will take appropriate steps to mitigate that risk.

The FOIPP Act authorizes government to use contractors to provide services involving even sensitive personal information as long as reasonable security arrangements are in place to protect that information.

- The FOIPP Act authorizes a public body to disclose any personal information to a contractor that is necessary for the contractor to perform the contracted services. At the same time, the Act requires public bodies to implement appropriate physical and procedural security measures with respect to personal information in its custody or control.
- It would not be appropriate therefore to conclude that the enactment of the *Patriot Act* renders B.C. public bodies unable, by virtue of their FOIPP Act obligations, to disclose personal information to service providers with U.S. connections. As always, the obligations under the FOIPP Act must be addressed on a case by case basis.
- As you and former Commissioner David Flaherty have both recognized, there is no such thing as absolute security. What the FOIPP Act requires is that there be security arrangements that a fair and rational person would consider to be proportionate to the sensitivity of the personal information.
- Given the small incremental risk of disclosure of Canadian information under the *Patriot Act*, the Province believes that disclosing sensitive personal information to a B.C. or Canadian company with U.S.

connections in the course of public body outsourcing would not contravene the security requirements of the FOIPP Act provided that a public body:

- Employs mitigation strategies to ensure that the B.C. or Canadian company's U.S. affiliate does not have access to, or control of, public body-supplied personal information that is held in Canada or B.C. These should prevent a U.S. company from being able to collect personal information held by its Canadian affiliate under the *Patriot Act*. Such mitigation strategies must be commensurate with the sensitivity of the personal information in question;
- Ensures that there are contractual provisions in place dealing with both privacy and security issues and that such provisions are commensurate with the sensitivity of the personal information in question; and
- Takes steps to minimize the extent to which any sensitive personal information is sent to the U.S. on a temporary or permanent basis. Government will not send sensitive personal information to the US either on a temporary or permanent basis.

The Province believes that there should be a national discussion about privacy.

- The Province will continue to work with the federal government to encourage Canada to affirm the international obligations of the United States with respect to information sharing, and receives appropriate assurances that existing established mechanisms will be used when Canadian information is required for security or law enforcement purposes.
- In this submission the Province will address existing U.S./Canada information sharing mechanisms; U.S. and British Columbia legal frameworks; the risk of access to Canadian information under the *Patriot Act*; international trade commitments; and proposed privacy protection measures to minimize the small incremental risk posed by the *Patriot Act*.

2. Existing Information Sharing and Access Mechanisms

It is simply wrong to contend that personal information held in Canada was not susceptible to access by U.S. law enforcement officials prior to the enactment of the Patriot Act.

2.01 Existing mechanisms for information sharing between Canadian and U.S. law enforcement agencies to deal with global threats to security and law enforcement predate the *Patriot Act* and are well established. Whether there is any added incremental risk posed by the *Patriot Act* requires consideration of such mechanisms as the Mutual Legal Assistance Treaty, grand jury subpoenas and less formal legally sanctioned information sharing processes.

2.02 The Province assessed several factors, including the existence of existing established mechanisms for information sharing, foreign governments' objections to U.S. attempts to extend the application or the effect of its laws extraterritorially and the cautious approach that the U.S. has exercised in response to those objections, as well as the domestic controversy that the *Patriot Act* has generated. The Province concludes that the risk that the U.S. will attempt to demand production of information held in Canada pursuant to the *Patriot Act* is small. The established processes for access to information held in Canada are described immediately below, followed by a discussion of the legal framework in section 3 and risk assessment in section 4.

The Mutual Legal Assistance Treaty

Under the Canada-U.S. Mutual Legal Assistance Treaty, U.S. authorities must first try to obtain records relating to a criminal investigation that are located in Canada through the assistance of Canadian authorities. The Mutual Legal Assistance Treaty contemplates the approval of the Canadian federal government and a Canadian court before production is ordered.

2.03 Partly because of concerns by other countries that the U.S. government not iassert its jurisdiction to compel the production of records held abroad, there now exist many Multilateral Legal Assistance Treaties involving the U.S. and other countries.

2.04 The U.S. and Canada signed a *Mutual Legal Assistance Treaty* on March 18, 1985, entered into force in Canada on January 24, 1990, to facilitate the cross-border production of documents more than a decade before the *Patriot Act* was

passed (the "MLAT").[1] That treaty is the primary method used by the U.S. government to obtain evidence located in Canada — whether held by a Canadian company, a Canadian individual, or Canadian governmental authorities.

2.05 The MLAT requires the parties to produce government-held documents "to the same extent and under the same conditions as would be available to [their] own law enforcement and judicial authorities".[2] This applies to "all levels of government, including federal, state, provincial, territorial, and municipal."[3] Thus, under the MLAT, U.S. law enforcement authorities can potentially access personal information held by the Province or other Canadian governments to the same extent that Canadian law enforcement and judicial authorities potentially have access to such information.

2.06 The Province notes that the FOIPP Act acknowledges that a public body can disclose personal information where authorized in accordance with a treaty made under an enactment of Canada or British Columbia (section 33(d.1)). As such, any disclosure of B.C. Government information required under the MLAT would be authorized by the FOIPP Act (with the "enactment" for the purposes of the FOIPPA being the federal *Mutual Legal Assistance in Criminal Matters Act* ("MLACMA")).

2.07 Under the MLAT, U.S. authorities *must* first try to obtain records located in Canada through the assistance of Canadian authorities. Specifically, Article IV states that "[a] [p]arty seeking to obtain documents, records or other articles known to be located in the territory of the other [p]arty *shall* request assistance pursuant to the provisions of this Treaty," except when the parties otherwise agree.[4] According to the official U.S. government Technical Analysis that accompanied the submission of the Treaty to the U.S. Senate, "[t]he United States agreed to this 'first resort' provision because *the scope of the Treaty is broad enough to cover the vast majority of situations requiring the production of documents and records located in Canada* and because the United States is convinced that the Treaty mechanism will provide the evidence in a timely manner."[5] The Canadian delegation, in turn, "considered this a matter of great

---

1 The MLAT was self-executing in the United States, utilizing existing statutory authority to become law. *See* Letter of Transmittal from Pres. Reagan ("Letter of Transmittal"), *reprinted in* S. Treaty Doc. 100-14, 100th Cong., 2d Sess. at iii (Feb. 22, 1988).

2 MLAT, art. XIII.

3 Technical Analysis, at 21.

4 MLAT, art. IV, § 1 (emphasis added).

5 Technical Analysis, Mutual Legal Assistance Treaty Between United States and Canada ("Technical Analysis"), *reprinted in* S. Treaty Doc. 100-14, 100th Cong., 2d Sess. at 13 (1988) (emphasis added). The Technical Analysis, which was prepared by the U.S. negotiating team for the Treaty, "constitutes the formal executive branch representation as to the meaning of [the] treaty and the obligations to be assumed by the United States under it[.]" *See* Senate Report, Treaty with Canada on Mutual Legal Assistance in Criminal Matters ("Senate Report"), *reprinted in* S. Treaty Doc. 100-14, 100th Cong., 2d Sess. at 5 (Sept. 30, 1988). As such, it serves as the principal U.S. guide to interpreting the Treaty. *See In re Commissioner's Subpoenas*, 325 F.3d 1287, 1298 (11th Cir. 2003) (citing *El Al Airlines, Ltd*

importance ... in order to regularize trans-border evidence gathering activities and to reduce the United States' enforcement of subpoenas [to obtain foreign-held evidence]."[6] The Province will refer extensively to the U.S. Technical Analysis in these submissions, because in dealing with the risk of the potential issuance of an order under the *Patriot Act* in relation to Canadian information, we need to understand U.S. law, including U.S. law concerning the MLAT.

2.08 Equally important as its "first resort" requirement, the MLAT provides for a broad range of cooperation on matters "relating to the investigation, prosecution and suppression of offences" in the requesting state, which, for the U.S., includes any "offence for which the statutory penalty is a term of imprisonment of one year or more . . . ."[7] This includes investigative assistance in obtaining documents, records and evidence, regardless of whether the "offence" being investigated would also be an offence in Canada.[8]

2.09 The MLAT has long effectively enabled prosecutors in the U.S. to seek a wide range of law enforcement assistance from Canadian authorities, including assistance in obtaining information during the investigative stage of a matter that might broadly be related to an "offense" in the U.S. The MLAT stipulates that it is to serve as the avenue of first resort for any attempt to obtain documents, records or other evidence held in the territory of the other country, sanctioning other methods only to the extent that MLAT proves unavailing. As such, the Province believes that, in most cases, the U.S. government would seek to obtain records held in Canada through the MLAT before resorting to seeking a *Patriot Act* order.

2.10 The MLAT offers certain procedural advantages over other law enforcement tools. Responsibility for making and executing requests under the Treaty is vested in the executive authorities of each country, namely the Canadian Minister of Justice and the U.S. Attorney General, or their designees.[9] Discretion to grant or deny assistance likewise is afforded to the executive, rather than the judicial, authorities of each country, but it may only be exercised on two grounds: (1) if the

---

v. Tsui Yuan Tseng, 525 U.S. 155, 168 (1999)) ("This official interpretation by the executive branch is entitled to great deference by [a] [c]ourt.").

6 Technical Analysis, at 13.

7 MLAT, art. I, art. II, § 1. In drafting the Treaty, the U.S. determined that this definition was "broad enough to cover all serious federal and state offenses." *See* Technical Analysis, at 11.

8 MLAT, art. II, §§ 2-3; Senate Report, at 3 (noting assistance under the MLAT "is available without regard to 'dual criminality'").
For U.S. authorities, this level of assistance is an important improvement over the pre-MLAT regime. Prior to the MLAT, a Canadian court reportedly "had authority to order production of documents . . . for a foreign country only if the court were satisfied that the evidence produced would be used at trial [i.e., the request was post-indictment] and that it was not sought solely for the purpose of furthering this investigation." Senate report, at 2-3. These qualifications to Canadian assistance led directly to the United States' reliance on the infamous "Bank of Nova Scotia subpoenas." *See id.* at 3 and discussion *infra* pp. 16-18.

9 *See* MLAT, art. I, art. VI, § 1.

request is not made in conformance with the Treaty; or (2) if execution of the request is contrary to the public interest of the state receiving the request.[10]

2.11 According to the U.S. Government's Technical Analysis, "a request should not be refused for inconsequential reasons". Examples of the kinds of cases the negotiators had in mind that would permit refusal of assistance include requests requiring disclosure of important military secrets or requests for assistance in a prosecution offensive to basic principles of society."[11] The court charged with enforcing the request in the state receiving the request "has inherent authority to satisfy itself that the Central Authority made its decision after fully considering all relevant issues," but it may not "substitute its discretion for that of the Central Authority."[12]

2.12 If a state wishes to exercise its discretion to deny a request for assistance under the MLAT, it must first consult with the requesting state to see if a satisfactory arrangement can be devised to permit assistance on other terms. If no arrangement can be reached after 30 days, the consultations will be considered terminated, and the parties' obligations under the Treaty will be deemed to have been fulfilled.

2.13 In negotiating the MLAT, both parties agreed that, once this consultative process had taken place without avail, it would not be considered a violation of the Treaty for the U.S. or Canada to resort to other means of compelling disclosure, including the issuance of subpoenas.

2.14 It is worth noting that the use of grand jury subpoenas by the U.S. to obtain foreign evidence (more detail on that issue to follow) has diminished in recent years and that the U.S. and Canada have increasingly relied on the MLAT[13]. This suggests that the U.S. and Canada have generally reached a mutually satisfactory arrangement under the MLAT.

2.15 The MLAT process includes provisions for notice and judicial oversight concerning the release of information.

2.16 The requirement to use MLAT covers the types of information contemplated by MLAT. The MLAT is a mechanism for exchanging information concerning criminal investigations. The *Patriot Act* contemplates obtaining information in connection with investigations of terrorism or clandestine intelligence activities. If, and to the extent that, these purposes are not co-extensive, the *Patriot Act* potentially allows U.S. authorities to obtain access to information in

---

10 *Id.*, art. V, § 1. "'Public interest' means any substantial interest related to national security or other essential public policy." *Id.*, art. I.

11 Technical Analysis, at 15.

12 *Id.*

13 *See* Thomas G. Snow, *The Investigation and Prosecution of White Collar Crime: International Challenges and the Legal Tools Available to Address Them*, 11 WM. & MARY BILL RTS. J. 209, 233 (2002).

circumstances under which they would not have had that access previously under the MLAT. However, the Province believes that that added risk is nominal on the basis of (1) the existence of other avenues for the lawful exchange of personal information between Canadian and U.S. law enforcement agencies (i.e., under the FOIPP Act and the federal *Privacy Act*), (2) the U.S. Government's reluctance in recent years to extend its powers extra-territorially to order the production of documents found within the borders of an ally, and (3) our belief that investigations under the *Patriot Act* will generally be of a criminal nature.

Canadian Implementation of MLAT

2.17 While in the US the MLAT is self-executing, in Canada the MLAT was implemented by statute. The MLACMA[14] is the federal statute that provides for the manner in which requests for legal assistance by the US (or other states that are party to an agreement with Canada) are to be addressed. Under that Act, a request is received for assistance to the Minister of Justice who is responsible for implementing and administering this Act and the relevant treaties (s. 7). Upon receipt of a request, the Minister of Justice must review the request to ensure that it complies with the relevant treaty (s. 8). The Act provides for *ex parte* applications for search warrants (ss. 10-14) and evidence gathering orders (ss. 17-19). The applications are to be made to a judge in the province or territory in which Canada believes part or all of the evidence may be found. The judge who hears the application may issue the warrant or order if the requirements of the Act are met (ss. 12 and 18).

2.18 Before evidence seized or produced is sent to the requesting state, the MLACMA requires a further court hearing to consider the execution of the warrant, at which a person claiming interest in the evidence may make representations. The court may impose conditions with respect to the sending abroad order and the Minister must be satisfied that the requesting state has agreed to comply with such conditions (ss. 12-16). With respect to evidence gathering orders, the MLACMA provides for a specified basis for refusals to comply with orders (s. 18(7)).

Summary

2.19 In sum, the MLAT provides a streamlined default process for authorities in the U.S. to obtain information held in Canada, and vice versa. The MLAT must be utilized by the requesting state in the first instance, and must be honoured by the state receiving the request except in limited circumstances. Even in the event a request is denied, the parties are required first to explore alternative means of cooperative assistance before resorting to unilateral measures such as subpoena powers and, presumably, orders under the *Patriot Act*.

The option of seeking a grand jury subpoena for access to records held abroad existed prior to the passage of the Patriot Act and prior to the signing of the MLAT and remains available to U.S. law enforcement agencies in the event the parties are unable to reach an agreement under the MLAT.

2.20 Obtaining business records is a long-standing law enforcement tactic in the U.S.. Ordinary grand juries for years have issued subpoenas to all manner of businesses, including libraries and bookstores, for records relevant to criminal inquiries.

2.21 The option of seeking a grand jury subpoena existed prior to the passage of the *Patriot Act* and prior to the signing of the MLAT and remains available to U.S. law enforcement agencies in the event the parties are unable to reach an agreement under the MLAT.

2.22 In the United States, grand juries serve a vital function for law enforcement authorities in investigating possible criminal conduct by providing prosecutors with the public's *imprimatur* on gathered evidence.[15] Through the issuance of subpoenas, grand juries have the power to require the production of evidence, books, papers, documents, data, or other objects related to a criminal investigation.[16] This power existed prior to the passage of the *Patriot Act*.

2.23 Notwithstanding the power of grand juries to issue subpoenas, U.S. law enforcement authorities are generally cautious about any extraterritorial extension of U.S. jurisdiction when they know that it will be objectionable to a close ally. Such attempts in the past have proven controversial, particularly where it related to sensitive documents protected by law from disclosure. As a result, the U.S. Department of Justice now requires its prosecutors to receive the approval of its Office of International Affairs ("OIA") before seeking what are colloquially termed "Bank of Nova Scotia subpoenas".

2.24 The test for production in the event one is served with a grand jury subpoena is one of control, not location."[17] Though we do not know for certain, by reason of the lack of available case law, the Province believes it is reasonable to presume that the same criteria will be applied in the case of applications under the *Patriot Act*. The term "control" includes not only physical possession and the "legal right

---

14 See supra, note 2.

15 *See Branzburg v. Hayes*, 408 U.S. 665, 688 (1972) (noting that basis for grand jury's subpoena power is "longstanding principle that the public . . . has a right to every man's evidence.") (citations and internal quotation marks omitted).

16 *See* FED. R. CRIM. P. 17(c)(1); *see also United States v. Mandujano*, 425 U.S. 564, 571 (1976).

17 *In re Marc Rich & Co., A.G.*, 707 F.2d 663, 667 (2d Cir. 1983).

to obtain the documents requested upon demand,"[18] but also "access to [the] documents and the ability to obtain them for [a company's] usual business."[19]

2.25 Grand jury subpoenas are not unlimited, and the subpoena "will be disallowed if it is far too sweeping in its terms to be regarded as reasonable under the Fourth Amendment."[20] Although there is no *per se* definition of "reasonableness," U.S. courts have acknowledged that "three interrelated requirements appear critical: (1) that the subpoena command only the production of materials relevant to the investigation; (2) that the subpoena specify the materials to be produced with reasonable particularity; and (3) that the subpoena command production of materials covering only a reasonable period of time."[21]

2.26 Assuming that a subpoena satisfies the foregoing requirements, the next question is whether the U.S. court would have the requisite constitutional jurisdiction to issue a subpoena. The jurisdictional reach of a subpoena extends as far as the jurisdiction of the court in which the grand jury sits. Foreign entities are thus subject to a grand jury subpoena only to the extent that they would otherwise be subject to the jurisdiction of the court.[22]

2.27 In the United States, constitutional due process requires that, in order for the court to have personal jurisdiction over a nonresident person or company, that person or company must have certain minimum contacts with the jurisdiction of the court in the United States. This is so that the exercise of jurisdiction does not "offend traditional notions of fair play and substantial justice.[23]

---

18 *Searock v. Stripling*, 736 F.2d 650, 653 (11th Cir. 1984).

19 *Cooper Indus., Inc. v. British Aerospace, Inc.*, 102 F.R.D. 918, 919-20 (S.D.N.Y. 1984); *see also United States v. IBM Corp.*, 71 F.R.D. 88, 91 (S.D.N.Y. 1976) (finding that board resolution threatening to discharge president if he complied with subpoena did not "deprive him of access and control" of documents, holding that such control is sufficient to require compliance with subpoena).

20 *United States v. Calandra*, 414 U.S. 338, 346 (1974) (citation and internal quotation marks omitted). The Fourth Amendment to the U.S. Constitution protects against unreasonable searches and seizures.

21 *In re Corrado Bros., Inc.*, 367 F. Supp. 1126, 1129 (D. Del. 1973) (citing *United States v. Gurule*, 437 F.2d 239, 241 (10th Cir. 1970)).

22 *In re Arawak Trust Co. (Cayman) Ltd.*, 489 F. Supp. 162, 165 (E.D.N.Y. 1980); *see also In re Marc Rich & Co., A.G.*, 707 F.2d 663, 669 (2d Cir. 1983), *cert. denied*, 463 U.S. 1215 (1983) ("A federal court's jurisdiction is not determined by its power to issue a subpoena; its power to issue a subpoena is determined by its jurisdiction."); *Fed. Trade Comm'n v. Compagnie de Saint-Gobain-Pont-A-Mousson*, 636 F.2d 1300, 1318 (D.C. Cir. 1980) ("When an American court orders enforcement of a subpoena requiring the production of documents and threatens penalties for noncompliance with that subpoena, it invokes the enforcement jurisdiction, rather than the prescriptive jurisdiction, of the United States. The two types of jurisdiction are not geographically coextensive[]. [A] state having jurisdiction to prescribe a rule of law does not necessarily have jurisdiction to enforce it in all cases, for unlike a state's prescriptive jurisdiction, which is not strictly limited by territorial boundaries, enforcement jurisdiction by and large continues to be strictly territorial.").

23 *See In re Arawak Trust Co. (Cayman) Ltd.*, 489 F. Supp. at 165 ("The court imputes to Congress a purpose to limit the court's personal jurisdiction to subpoena a foreign corporation to the kind of circumstances discussed in *International Shoe Company v. Washington*, 326 U.S. 310 (1945)."). See also, for example, *In re Sealed Case*, 266 U.S. App. D.C. 30; 832 F.2d 1268.

2.28 In the case of Canadian companies that do not regularly do business in the U.S., jurisdiction may be founded on conduct abroad that causes injury within the United States. In general terms, a Canadian company might also be subject to the general jurisdiction of a U.S. court when it possesses "continuous and systematic" contacts with the U.S.. If neither of these scenarios apply, generally the United States court will not have personal jurisdiction over a Canadian company.[24]

2.29 Generally, a Canadian foreign company is not subject to the jurisdiction of the U.S. court simply because its corporate affiliate is doing business there.[25]

2.30 Notwithstanding the power of grand juries to issue subpoenas, U.S. law enforcement authorities are generally cautious about any extraterritorial extension of U.S. jurisdiction when they know that it will be objectionable to a close ally. On this point, the *Bank of Nova Scotia* line of cases from the 1980s, and the U.S. Department of Justice guidelines that ensued, are illustrative.

2.31 *In re. Grand Jury Proceedings (Bank of Nova Scotia)* involved the U.S. government's use of grand jury subpoenas to compel a U.S.-branch of the Bank of Nova Scotia to produce documents held by branches in the Bahamas and the Cayman Islands, even though production of the records violated the secrecy laws of those countries.[26] This extraterritorial assertion of U.S. jurisdiction proved controversial, particularly because it related to sensitive documents that commonly are protected under bank secrecy laws. As a result, the U.S. Department of Justice now requires its prosecutors to receive the approval of the OIA before seeking what are colloquially termed "Bank of Nova Scotia subpoenas". The U.S. Department of Justice guidance on this issue states:

"Under modern doctrine, due process is not satisfied unless the [individual or entity] has sufficient 'minimum contacts' with the forum" such that the exercise of jurisdiction "does not offend 'traditional notions of fair play and substantial justice.'" *Compagnie de Saint-Gobain-Pont-A-Mousson*, 636 F.2d at 1319 (citing *Shaffer v. Heitner*, 433 U.S. 186 (1977) and *Int'l Shoe v. Washington*, 326 U.S. 310 (1945)).

24 See *Exter Shipping, Ltd. v. Kilakos*, 310 F. Supp. 2d 1301 (2004) for a recent summary of the law pertaining to personal jurisdiction.

25 *Exter Shipping, Ltd. v. Kilakos*, supra ("..It is well established... that when a parent and a subsidiary are separate and distinct corporate entities, the presence of one in a forum state may not necessarily be attributed to the other....Generally, a foreign parent corporation is not subject to the jurisdiction of a forum state simply because its subsidiary is doing business there....Rather, where the subsidiary's presence in the state is primarily for the purpose of carrying on its business and the subsidiary has preserved some semblance of independence from the parent, jurisdiction over the parent may not be acquired on the basis of the local activities of the subsidiary.")

26 *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817, 827-29 (11th Cir. 1984) (noting that the law of secrecy in the Cayman Islands "does not operate as a blanket guarantee of privacy and has many exceptions" and finding enforcement of the subpoena to be "consistent with the grand jury's goals of investigating criminal matters"); *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 691 F.2d 1384, 1391 (11th Cir. 1982) (ordering enforcement of subpoena, finding that "a grand jury's investigative function" outweighs "the Bahamas' interest in the right of privacy," and noting that "[a] Bahamian court would be able to order production of these documents").

> [F]oreign governments strongly object to such subpoenas, contending that they constitute an improper exercise of United States jurisdiction. Though the issue has arisen in connection with corporate entities, these concerns are equally applicable to a subpoena directed at an individual where the demanded production of evidence located in the territory of another country would violate that country's laws.
>
> Since the use of unilateral compulsory measures can adversely affect the law enforcement relationship with the foreign country, all federal prosecutors must obtain written approval through OIA before issuing any subpoenas to persons or entities in the United States for records located abroad.
>
> ...
>
> OIA must also be consulted prior to initiating enforcement proceedings relating to such subpoenas.[27]

With the increasing number of orders under the MLAT that provide a less coercive and less controversial means to obtain foreign records, the need for the U.S. to resort to "Bank of Nova Scotia subpoenas" has diminished.

2.32 "Bank of Nova Scotia subpoenas" are generally viewed by foreign governments as an improper assertion of extraterritorial power by the United States which infringes upon state sovereignty. The use of those subpoenas has sometimes led to diplomatic criticism and complaints. That is why U.S. federal prosecutors must obtain approval from the OIA prior to issuing or enforcing such subpoenas. With the increasing number of orders under the MLAT that provide a less coercive and less controversial means to obtain foreign records, the need for the U.S. to resort to "Bank of Nova Scotia subpoenas" has diminished.[28]

2.33 A further factor that will be considered by the OIA is whether the need to protect against the destruction of records justifies issuing a subpoena.[29] It is hard to imagine how this consideration would apply with respect to information held by Canadian or British Columbia service providers.

2.34 While the MLAT now provides the primary means of obtaining records located in Canada, the United States still maintains the right to utilize grand jury subpoenas in the event the Treaty process breaks down,[30] as long as the records fall within the control of a U.S. parent or affiliate, or the Canadian entity holding the records is subject to jurisdiction and service of process by the U.S. court, although it

---

27 United States Department of Justice Criminal Resources Manual, Title 9, § 279 (Oct. 1997), *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00279.htm.

28 Ibid, page 233.

29 *Ibid*

30 *See* Technical Analysis, at 13 (discussing Article IV or the Treaty, and noting that enforcement of such a subpoena is permitted after the consultative process required by the Treaty has taken place).

would apply OIA policy, in making such a determination. Presumably, the same considerations would apply with respect to an order under the *Patriot Act*.

Other U.S. and Canada Law Enforcement Information Sharing Mechanisms

There exist many lawful information sharing mechanisms that allow Canadian law enforcement agencies to exchange information with law enforcement agencies in other countries. They recognize that crime - and terrorism - crosses borders routinely.

Such established processes to acquire personal information held abroad are much more likely to be used by U.S. law enforcement agencies than an application under the Patriot Act, given the reluctance of the U.S. to extraterritorially extend its jurisdiction to records found in the territory of a close ally, of which Canada is one.

2.35 There exist many information sharing processes outside of the *Patriot Act* that allow law enforcement agencies in different countries to lawfully exchange personal information required to investigate criminal and terrorist activities.

2.36 If law enforcement is to be effective, law enforcement officials need processes and mechanisms within which information legitimately necessary for investigation and enforcement can be exchanged. Because the sharing of personal information under existing legally sanctioned processes does not require obtaining a court order, whereas access under the *Patriot Act* does, the Province believes that such established processes to acquire personal information held abroad are much more likely to be used by U.S. law enforcement agencies than an application under the *Patriot Act*, given the reluctance of the U.S. to extraterritorially extend its jurisdiction to records found in the territory of a close ally, of which Canada is one.

2.37 The Province believes that the existence of such existing, legally sanctioned, information sharing processes is another factor weighing in favour of a finding that the incremental risk of access to Canadian personal information posed by the *Patriot Act* is minimal.

2.38 The Province notes that the *FOIPP Act* itself contemplates that personal information can be shared with law enforcement agencies of a foreign country in certain circumstances. Section 33(o) of the *FOIPP Act* provides that a public body that is a law enforcement agency may disclose to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority.

2.39 Similarly, s. 8(2)(f) of the federal *Privacy Act, R.S.* 1985, c. P-21, provides that, subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed

> (f) under an agreement or arrangement between the Government of Canada or an institution thereof and the government of a province, the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation.

2.40 The Province believes that existing U.S.-Canada personal information sharing mechanisms between U.S. and Canadian law enforcement agencies are relevant to a determination as to what incremental privacy risk is posed to Canadian information by the U.S.A. *Patriot Act*. The following Canadian and B.C. statutes authorize such mechanisms;

- Information sharing agreements between Canadian and foreign law enforcement agencies, as authorized by section 33 (o) of the FOIPP Act and section 8(2)(f) of the federal *Privacy Act*. For instance, the Province understands that the RCMP has entered into information sharing agreements with law enforcement agencies outside of Canada, including the FBI. In addition, Interpol, of which Canada is a part, is an organization that facilitates information sharing amongst law enforcement agencies in different countries.

- Sections 33(c) of the FOIPP Act and 8(2)(a) of the federal *Privacy Act* authorize federal and provincial domestic law enforcement agencies to disclose personal information to U.S. law enforcement agencies, including the FBI, where the "consistent use" test is met. Such disclosures can be made outside of the MLAT process without applying for an order under the *Patriot Act*. If a U.S. law enforcement agency requests personal information from a Canadian law enforcement agency and the latter believes that there is a legitimate Canadian investigative interest involved, but there is no existing information sharing agreement in place, and they have access to the requested information, the B.C. or Canadian agency has the authority to disclose such information under sections 33(c) of the FOIPP Act or 8(2)(a) of the federal *Privacy Act*, whichever is applicable. The Province refers the Commissioner to Appendix "A" which lists the personal information banks of the RCMP. That list refers to information in some banks that is shared with foreign law enforcement agencies.[31] In addition, "Integrated National Security Enforcement Teams" (INSET's), made up of federal, provincial and municipal law enforcement agencies, have been formed to combat national security threats. Those INSET's permit the RCMP to work with international partners to share intelligence information.[32]

---

31 That document was found at the following website; www.infosource.gc.ca.

32 INSET's are described in a webpage found in the Province's list of authorities, which was found on the RCMP website, www.rcmp-grc.gc.ca.

- Section 17(1)(b) of the *Canadian Security Intelligence Service Act* (the "CSIS Act") authorizes the Canadian Security Intelligence Service (CSIS) to enter into information sharing contracts. That subsection reads:

> **17.** (1) For the purpose of performing its duties and functions under this Act, the Service may
>
> ...
>
> (*b*) with the approval of the Minister after consultation by the Minister with the Minister of Foreign Affairs, enter into an arrangement or otherwise cooperate with the government of a foreign state or an institution thereof or an international organization of states or an institution thereof.

The Province refers the Commissioner to Appendix "B" of these submissions which lists the personal information banks of CSIS, which references personal information being shared with foreign agencies under section 17 of the *CSIS Act*.

3. Legal Framework

The British Columbia Freedom of Information and Protection of Privacy Act ("the FOIPP Act"),

Under the FOIPP Act, public bodies must make sensible, proportional and reasoned arrangements to ensure the safety of personal information within their custody or control.

3.01 Section 30 of the FOIPP Act provides that the head of a public body must protect personal information in the custody or under the control of the public body by making reasonable security arrangements against such risks as unauthorized access, collection, use disclosure or disposal.

3.02 The FOIPP Act applies to records in the custody or under the control of a public body. Provincial ministries are included with the FOIPP Act's definition of "public body". As such, when a ministry outsources data management functions to a third party, section 30 of the FOIPP Act requires that it make "reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal" of any personal information it provides to the contractor.

3.03 The Oxford New English Dictionary provides the following definition of "reasonable", in part:

> "...1. Endowed with the faculty of reason, rational...2. In accordance with reason; not irrational or absurd...3. Proportionate... 4. Having sound judgement; ready to listen to reason, sensible. Also, not asking for too much..5. Within the limits of reason; not greatly less or more than might be thought likely or appropriate; moderate...."

That definition supports a finding that the "reasonable" standard in section 30 is not one that requires perfection. Rather, the obligation to make "reasonable" security arrangements requires that sensible and proportionate arrangements be made against such risks as unauthorized access, collection, use, disclosure or disposal.

3.04 Black's Law Dictionary defines "reasonable" as follows:

> *" Fair, proper, just, moderate, suitable under the circumstances. Fit and appropriate to the end in view...Not immoderate or excessive, being synonymous with rational, honest, equitable, fair, suitable, moderate, tolerable."*

3.05 The Alberta Information and Privacy Commissioner accepted the above definition in Order No. 98-002, with particular emphasis on "fair" and "suitable under the circumstances".

3.06 The Oxford New English Dictionary provides the following definition of "security", in part:

> "... 1. The condition of being protected from or not exposed to danger; safety; spec. the condition of being protected from espionage, attack, or theft. Also, the condition of being kept in safe custody ... the provision or exercise of measures to ensure such safety".

Reasonable security arrangements do not require absolute or perfect security. They are what a fair and rational person would consider appropriate, having regard to the sensitivity of the information.

3.07 In interpreting the "reasonable" security arrangements requirement in section 30, it is helpful to consider previous decisions of the Commissioner that deal with another section of the FOIPP Act that imposes a "reasonable" standard. Section 6 of the FOIPP Act provides that the head of a public body must make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely. Consistent with the above definition of "reasonable", the Commissioner has held that the "reasonable" requirement in section 6 does not require perfection. In paragraph 14 of Order No. 02-03 the Commissioner stated as follows;

> "...Although the Act does not impose a standard of perfection, it is well established that, in searching for records, a public body must do that which a fair and rational person would expect to be done or consider acceptable..."

3.08 Similarly, the Province submits that the reference to "reasonable" in section 30 means that that section also does not impose a standard of perfection. As such, section 30 does not require public bodies to demonstrate that security lapses in relation to personal information in its control will never, under any circumstances, occur. Rather, a public body is required to make "reasonable" security arrangements against such risks.

3.09 Commissioner Flaherty has noted that there is no such thing as "absolute security".[33] You have similarly stated that "risk can never be eliminated".[34] One can never be sure that security breaches will never happen in the future.

3.10 The Province submits that a public body is not obligated to undertake extreme measures to eliminate every negligible or remote security risk, but rather to implement security arrangements that a fair and reasonable person would consider appropriate, in the circumstances, to try to prevent unauthorized access.

---

33 "The British Columbia Cancer Agency: The Results of a Privacy Check-Up"

34 "Identity, Privacy & Security—Can Technology Really Reconcile Them?"

3.11 The Government's *Freedom of Information and Protection of Privacy Act Policy and Procedures Manual* currently provides the following guidance with respect to the "reasonable security arrangements" requirement under section 30;

> For public bodies not covered by CORE, "reasonable security arrangements" are those which a fair, rational person would think were appropriate to the sensitivity of the information and to the medium in which it is stored, transmitted, handled, or transferred. A sliding scale of security arrangements is appropriate, depending on the sensitivity of the personal information that a public body handles.

3.12 The Commissioner's office has cited the reference in the *Freedom of Information and Protection of Privacy Act Policy and Procedures Manual* to the "fair and rational person test" in the 1996 document entitled *"Guidelines for the Secure Transmission of Personal information by Fax"*,

> "The *Freedom of Information and Protection of Privacy THE FOIPP ACT* Policy and Procedures Manual defines reasonable security arrangements for personal information in the custody or under the control of public bodies. They are arrangements which fair and rational people would think are appropriate to the sensitivity of the information and to the medium in which it is stored, transmitted, or handled."

3.13 As mentioned, the definition of "reasonable" includes within it the notion of "proportionate". As such, the Province submits that any security arrangements made by a public body should be proportionate to the level of risks involved and the sensitivity of the personal information in question (i.e. health information will require stronger security safeguards than many other types of personal information). As we have stated elsewhere, the Province is prepared to implement any reasonable security arrangements to protect government information.

Procedural and Physical Security Measures

> ***Public Bodies must protect personal information by using physical and procedural security measures that are appropriate to the sensitivity of the personal information.***

3.14 The Commissioner has dealt with the issue of security in the context of ensuring the physical and procedural security of personal information, including ensuring that employees are appropriately educated about confidentiality issues. For instance, the Commissioner stated as follows in Investigation Report P98-012:

> "Public bodies must protect personal information by using security safeguards appropriate to the sensitivity of the information. Section 30 requires the head of a public body to provide appropriate *physical and procedural security* measures to protect personal information in the custody or under the control of the public body." *(emphasis added)*

3.15 In "The British Columbia Cancer Agency: The Results of a Privacy Check-Up", the Commissioner reviewed the security practices of the British Columbia Cancer Agency. In that report, Commissioner Flaherty recognized that a public body is entitled to some leeway in developing processes and practices to ensure the security of its information, keeping in mind the needs of the public body and its clientele to deliver services effectively. The Commissioner stated as follows:

> "While my "recommendations" in this essay are just that, I have the authority to order appropriate changes if my recommendations are not followed, absent persuasive arguments to the contrary. Although my general practice is to defer to the judgment of professionals and specialists as to what is necessary and practical in terms of current practices, a number of my observations at the Vancouver Centre Hospital require specific changes to current practices. *But I also accept that fair information practices need to be consciously fashioned, by written policies, to the needs of public bodies and their clientele to deliver services effectively. Privacy protection is about balancing competing interests.*" (Emphasis added)

3.16 That acknowledgement by Commissioner Flaherty that privacy protection entails some balancing with other interests is a recognition that other social and public interests may legitimately be considered in any determination as to what constitutes "reasonable" security arrangements.

3.17 The word "reasonable" was presumably included in section 30 for a reason, namely, so as not to be interpreted as imposing obligations on a public body to make every possible security arrangement to prevent unauthorized access, collection, use, disclosure or disposal, regardless of the level of risk and regardless of the costs of implementing such arrangements. Firstly, it may not be "reasonable" in a given situation to devote additional resources to mitigate a risk that is already negligible. As such, the Province submits that a relevant factor in any section 30 analysis is the magnitude of the risk. Secondly, from a financial point of view, public bodies must operate within a fixed budget. For that reason, public bodies simply will not have sufficient financial and/or human resources to acquire and implement each and every available security asset and process, regardless of cost. As such, the Province submits that another relevant factor in any section 30 analysis is the financial and human resources available to a public body to implement security arrangements.

3.18 In addition, the Province submits that another relevant consideration in determining which procedural and physical measures should be implemented in a given situation is the operational requirements of a public body (i.e. providing effective client services, delivering programs and/or fulfilling its statutory mandate). For instance, incurring such costs may have potential adverse impacts on the public body's ability to deliver services or perform its functions.

3.19 As such, the Province submits that any finding that a public body has not met the requirements of section 30 will not warrant an order that the public body can no longer disclose personal information to a contractor (provided it has the authority

under section 33 to disclose the personal information in the first place). Rather, the Province respectfully submits that any such finding will only warrant an order requiring a public body to implement such additional physical and procedural security measures as are appropriate in the circumstances.

The Disclosure of Personal Information to Contractors

Public Bodies are permitted to share personal information for the purpose of outsourcing its functions or activities.

3.20 By virtue of the combined operation of sections 30 and 33, it is clear that a public body has the right to disclose personal information to a contractor when a public body outsources its functions to a third party. It must impose reasonable obligations in the contract concerning the physical and procedural security of personal information in its control, in order to ensure that any personal information supplied to the contractor and within the public body's control is not used, disclosed or disposed by the contractor contrary to sections 26 to 36 of the FOIPP Act. As such, the issue for the Commissioner to determine in a particular case, in the context of the *Patriot Act* issue, is what physical and procedural security arrangements must be imposed on a contractor with U.S. connections in order to ensure "reasonable security".

3.21 Section 30 of the Act requires public bodies to make reasonable security arrangements against the "unauthorized" disclosure of personal information. An "unauthorized disclosure" is a disclosure that is not authorized by the *FOIPP Act*. As such, in interpreting the duty under section 30, we need to consider section 33 of the FOIPP ACT, the section that cites the situations where a public body can lawfully disclose personal information in its custody or control.

3.22 Section 33 of the FOIPP Act provides that a public body may disclose personal information in its custody or control in the situations enumerated. That section reads as follow, in part (the full text of that section is found in Appendix "C").

> ...
>
> (f) to an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer, employee or minister,
>
> ...

3.23 Section 33(f) of the FOIPP Act allows a public body to disclose personal information to an "employee" where the information is necessary for the performance of the duties of that employee.

3.24 The FOIPP Act defines an "employee" in relation to a public body as including "a person retained under a contract to perform services for the public body".

3.25 "Person" is not defined under the FOIPP Act. However, it is defined under the British Columbia *Interpretation Act* as including "a corporation, partnership or party, and the personal or other legal representatives of a person to whom the context can apply according to law".

3.26 As such, where a public body enters into an agreement with an individual or a corporation for the provision of services, section 33(f) of the FOIPP Act authorizes a public body to disclose any personal information to the contractor that is necessary for the contractor to perform the contracted services. As such, section 33(f) of the FOIPP Act permits public bodies to share personal information for the purpose of outsourcing their functions or activities.

3.27 Accordingly, the Office of the Information and Privacy Commissioner's "Investigation into BC Nurses' Union Complaint about Telus-VGH LastWord Contract" states as follows:

> [76] Disclosure of personal information to contractors, subcontractors and their respective employees is permitted where the disclosed information is necessary for the performance of the duties of the employee (s. 33(f)). Schedule 1 to the Act defines "employee" as including a person retained under a contract to perform services for the public body. The Act, therefore, contemplates disclosure to contractors of personal information on a need-to-know basis in relation to performance of their services for a public body. A public body such as Vancouver Hospital should, however, expressly limit such disclosures, which has been done in s. 6.1 of the Contract.

3.28 The Legislature, by virtue of passing section 33(f) of the FOIPP Act, clearly intended that public bodies should be able to share personal information for the purpose of outsourcing its functions or activities.

Common sense dictates that a public body can never be completely certain at the time it enters into the contract that the terms of the contract (including terms pertaining to privacy and security) will never, under any circumstances, be breached, just as a public body can never be sure, despite its own privacy policies and procedures, that all of its employees will follow such procedures at all times. Again, there is no such thing as perfect security, regardless of whether we are dealing with information in the hands of a public body or of a contractor.

3.29 The Province submits that it is reasonable to conclude that it was not the intent of the Legislature that a public body could only share personal information with a contractor (per section 33(f)) where it was absolutely certain that the contractor would never, under any circumstances, disclose personal information in contravention of the FOIPP Act. If that were the case, a public body would never be able to share personal information to a contractor given that there can never be perfect security. As such, the Province submits that interpreting section 33(f) in

such a manner would be contrary to the clear intent of section 33(f) and the definition of "employee". Moreover, a modern rule of statutory interpretation is that it is presumed that legislation is not intended to produce absurd consequences. Further, absurdity is not limited to logical contradictions; it includes violations of reasonableness and common sense.[35] The Province submits that it would be both unreasonable and absurd to interpret section 33(f) as imposing a requirement that disclosure to a contractor can only occur where absolute security can be assured or the basis that such a standard could never be reached.

3.30 Section 33 of the FOIPP Act imposes obligations on a public body with respect to personal information that it controls but does not have custody of (i.e. where a third party obtains possession of the personal information on behalf of the public body and/or retains the right to access such information at any time). As such, the FOIPP Act contemplates that where a public body has properly disclosed personal information to a third party, but still exercises control over that information, the public body has a duty under section 33 to take reasonable efforts to ensure that such information is only disclosed in compliance with that section. In the past, the Commissioner has stated that the principal way to achieve that goal is to incorporate appropriate security and privacy language in the contract. A public body can do its best to ensure that the contract has appropriate terms dealing with privacy and security and can, through administering the contract, do its best is ensure that the contractor abides by the terms of the contract.

Disclosure of Personal information to Comply with a Subpoena, Warrant or Order

When a public body contracts with a company with U.S. connections, it must make reasonable security arrangements to ensure that any personal information disclosed to the company does not get disclosed for the purposes of the Patriot Act.

3.31 Section 30 imposes an obligation on a public body, where it contracts with a company with U.S. connections, to make reasonable security arrangements to ensure that any personal information disclosed to the company does not get disclosed for the purposes of the *Patriot Act*.

3.32 A public body may disclose personal information under section 33(e) of the FOIPP Act for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information.

---

[35] "Driedger on the Construction of Statutes", Third Edition by Ruth Sullivan (1994: Butterworth's) , page 85.

3.33 Does section 33(e) of the FOIPP ACT permit disclosure for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body outside of Canada? The Province submits that it does not. Of significance is that where the FOIPP Act refers elsewhere to disclosures being authorized by an enactment, it refers only to enactments of British Columbia or Canada. There is no reference in the FOIPP Act to a public body being able to disclose personal information where a foreign enactment authorizes such a disclosure.

Sensitivity of the Personal Information

There is no "one size fits all" solution in ensuring the reasonable security of personal information. **The issue in a particular case is what steps should reasonably be taken to ensure the security of personal information in the circumstances. Each case must be determined according to its particular facts, including the sensitivity of the data and the nature of the service-delivery relationship.**

3.34 In *R. v. Mills* (1999), the Supreme Court of Canada observed that the interest in being left alone by the state includes the ability to control the dissemination of confidential information. The court in *Mills* also referred to the sensitivity of information as being relevant to the issue of the expectation of privacy and said:

> "... privacy concerns are at their strongest where aspects of one's individual identity are at stake, such as in the context of information 'about one's lifestyle, intimate relations or political or religious opinions."

3.35 The Commissioner has recognized that, in dealing with privacy issues under Part 3 of the FOIPP ACT, one must consider the facts of each case. For instance, in OIPC Guideline 01-01, the Commissioner said:

> "Each case differs, of course. A variety of circumstances – including the nature of the personal information involved and the uses for that information – will determine which measures are necessary in each case to protect personal privacy and ensure the security of personal information. For example, a self-governing body need not, in creating and using a list of members' names and addresses, take the same measures for the privacy and security of that limited personal information, as a hospital would have to take respecting patients' personal medical information. These guidelines are, therefore, to be used as a common sense guide in light of the circumstances of each case."

3.36 In deciding what privacy protection measures should be taken by a public body to reduce the risk of unauthorized disclosure by its service provider, including under the USA *Patriot Act*, one must consider the sensitivity of the personal information in question.

3.37 The Commissioner has stated as follows in Investigation Report P98-012:

> "Public bodies must protect personal information by using security safeguards appropriate to the sensitivity of the information."

3.38 In addition, the Commissioner's office has issued "Guidelines For the Secure Transmission of Personal information by Fax", wherein the following statement is found;

> "Not all information held by public bodies requires the same degree of security when communicated from one source to another. Therefore, the first step for public bodies is to categorize the various types of information they hold. The appropriate degree of security will depend on the sensitivity and volume of personal information that a public body handles. Public bodies should conduct risk analysis on the types of information transmitted or received by fax. A particular branch, or entire public body, that faxes sensitive or confidential personal information may become classified as "high risk." Such high risk entities should be provided with extra secure fax capabilities."

3.39 In addressing the "reasonable security" issue, it is also relevant to consider whether the personal information in question is already publicly accessible. For instance, if we dealing with personal information that is already available through public registries and/or publicly available documents, lesser security measures will be required.

Other Relevant Factors in Addressing the "Reasonable Security" Issue

In determining what constitutes reasonable security arrangements, one must consider the tangible benefits of outsourcing public body functions, including reducing costs for government and improving the quality of services to the public.

It is reasonable for public bodies to expect that Canadian entities will obey their Canadian legal obligations.

3.40 As mentioned, the previous Commissioner, David Flaherty, stated that "privacy protection is about balancing competing interests." Accordingly, the Province submits that it is relevant to consider the tangible benefits of contracting out to a U.S. related company in a particular situation (i.e. financial benefits and/or operational or client service benefits). Alternatively, it will be relevant to consider any tangible disadvantages in a public body confining oneself to companies with no U.S. connections.

3.41 As such, the Province submits that any determination as to whether outsourcing initiatives complies with section 30 of the FOIPP Act must consider the benefits of such initiatives including;

- Increasing operational flexibility; For instance, a private company may be able to provide better operational flexibility through access to a wider range of skills and experience than public bodies have, or can afford, and an increased ability to respond to operational demands;
- The benefit of transferring risks to the private sector, such as system development risks and the costs of overruns, and service level risks;
- Making the best use of the limited resources available to a public body;
- Improving client service;
- Reducing operating costs;
- Transferring the costs of asset acquisition;
- The ability to focus on the core business of the public body;
- Cost certainty;
- Potential improvements in management reporting; the private sector can potentially provide improvements in the quantity, quality and timeliness of management reporting available for operational decision making; and
- Avoidance of significant future capital costs.

3.42 Often, private sector organizations have extensive security expertise in managing personal information. In addition, if a third party already has superior security processes or technology in place because it provides such services for other customers, it may be easier and less expensive for them to provide such services for a public body than it would be for a public body to go to the expense of investing in and incorporating such practices.

3.43 If public bodies were required to restrict outsourcing to companies with no U.S. connections, that could potentially hinder efforts to make reasonable security arrangements. By doing so, one would be excluding companies that offer significant expertise and experience in relation to managing large databases and ensuring the security of such systems. As such, there may be cases where contracting with a U.S. related company provides the best security of government data, despite the minimal risk of access to information under the *Patriot Act*.

3.44 An underlying premise of some opponents to government outsourcing is that government information will be safer with government employees than with a private company. However, a well-managed private sector firm with equivalent or superior security and confidentiality processes can potentially provide equal or better security. A private sector partner will be motivated to do a good job of ensuring the security of its information. Private sector entities have to compete in

the market place. When companies deal with personal information there is considerable incentive to make information secure. To do otherwise would create increased potential for privacy breaches, with the risk that customer confidence may be affected, a competitive advantage being lost or business may be lost.

3.45 The Province further submits that it is also reasonable for public bodies to presume that companies in British Columbia will abide by their legal obligations.[36] A requirement of any outsourcing contract will be that the service provider cannot disclose personal information in contravention of the FOIPP Act. While a public body can never be completely confident that a service provider will always abide by the terms of its contract, the Province submits that it would be unreasonable for a public body to initially presume that a Canadian service provider will fail to comply with its Canadian legal obligations.

The Patriot Act

The *Patriot Act is a U.S. response to concerns about international crime and terrorism, heightened as a result of the events of September 2001.*

3.46 US. President George W. Bush signed the *Patriot Act* into law on October 26, 2001. That Act was a swift legislative response to the month-earlier terrorist attacks, and expanded and established a variety of authorities related to U.S. homeland security. That Act made a number of amendments to the *Foreign Intelligence Surveillance Act* ("FISA").

3.47 FISA was originally enacted in 1978 to enable US intelligence and law enforcement agencies to conduct electronic surveillance of foreign powers in the US while complying with the constitutional provisions that regulate domestic law enforcement surveillance under the US federal wiretap statute. FISA was amended in 1994 to include covert physical entries, and in 1998, to provide the original authorization for access to certain business records. Three years thereafter, s. 215 of the Patriot Act in turn broadened the scope of records, entities and circumstances potentially subject to a FISA order.

3.48 Among the *Patriot Act*'s provisions, several sections enhanced foreign intelligence and law enforcement surveillance and investigative authorities.

---

[36] The Supreme Court of Canada in *Application under s. 83.28 of the Criminal Code (Re)*, [2004] S.C.J. No. 40, reads as follows at para. 5:

"The challenge for democracies in the battle against terrorism is not whether to respond, but rather how to do so. This is because Canadians value the importance of human life and liberty, and the protection of society through respect for the rule of law. Indeed, a democracy cannot exist without the rule of law. So, while Cicero long ago wrote '*inter arma silent leges*' (the laws are silent in battle): Cicero, *Pro Milone* 14, we, like others, must strongly disagree: see, A. Barak, 'Foreward: a Judge on Judging: The Role of a Supreme Court in a Democracy' (2002), 116 *Harv. L. Rev.* 16, at p. 150-51."

3.49 Of particular relevance, section 215 expanded the authority of the U.S. government to obtain business records in connection with investigations of terrorism or clandestine intelligence activities, as well as for the purpose of obtaining foreign intelligence information.[37] Powers are provided to the Federal Bureau of Investigation under the FISA. Section 215 is subject to a sunset clause of December 31, 2005.

3.50 Under s. 215 of the *Patriot Act*:

- the FBI may require the production of "tangible things" pertaining to anyone, provided that the information sought is related to an investigation to obtain foreign intelligence information or to protect against international terrorism or clandestine intelligence activities.

- The FBI may only do so where it first receives an order from a special court, the Foreign Intelligence Surveillance Court. Any such order granted by that court does not specify its purpose. Nor is a person served with a section 215 order allowed to disclose the fact that they have received the order, other than as necessary to produce the items sought.[38] The *Patriot Act* does not provide for an express penalty for non-compliance with an order issued under s. 215. However, it is presumed that if someone served with such an order does not comply, they could face contempt of court sanctions.[39]

---

37 *See* 50 U.S.C. § 1861.

38 *See* 50 U.S.C. § 1861(c)(1)-(2). Few sources address how the FISA process actually works in practice, largely because the FISA court issues a written opinion only when it denies an application. *See* 50 U.S.C. § 1803(a). Indeed, in its quarter-century of existence, the court has only denied one FISA application and consequently has issued just one opinion. *See* Edward Lee, *The Public's Domain. The Evolution of Legal Restraints on the Government's Power to Control Public Access Through Secrecy or Intellectual Property*, 55 Hastings L.J. 91, 94 (2003) (citing *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611 (Foreign Int. Surv. Ct. 2002)). This opinion was made public three months after it was issued. *See id.* Notably, the case involved an application for electronic surveillance, not a production order, and the court's denial was reversed by the Court of Review, which also published its first opinion in its first ever ruling. *See id.* at 95 (citing *In re Sealed Case*, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002)).

39 *See* 18 U.S.C. § 401(3) ("A court of the United States shall have power to punish by fine or imprisonment, or both . . . such contempt of its authority [as] . . . [d]isobedience or resistance to its lawful writ, process, order, rule, decree, or command.").

The Bush Administration attempted to make explicit this sanction in draft legislation captioned as the "Domestic Security Enhancement Act of 2003," which was disclosed to the public last year and eventually dubbed "Patriot II." A draft of the section-by-section analysis of "Patriot II" stated that:

> [I]f a person refuses to comply with . . . an order to produce records under 50 U.S.C. § 1861, existing law provides no clearly defined recourse to secure compliance with the court's order. This section remedies this omission by providing that the Foreign Intelligence Surveillance Court has the same authority as a United States district court to enforce its orders, including the authority to impose contempt sanctions in case of disobedience.

Analysis of Domestic Security Enhancement Act of 2003, p. 3 (Jan. 9, 2003 draft). The legislation was never introduced in Congress and has not been enacted into law.

3.51 Section 215 expanded the U.S. government's ability to collect records held in the private sector in different ways.

3.52 First, section 215 expanded the scope of records subject to production under a FISA order. The previous version of FISA applied only to "*records* in [the] possession" of an entity served with a FISA order.[40] However, under section 215, the scope of production now encompasses "*any tangible things* (including books, records, papers, documents, and other items),"[41] and there no longer is a statutory requirement that such items be in the "possession of" the served entity.

3.53 Second, section 215 expanded the range of entities upon whom a FISA production order can be made. Previously, a FISA production order could be served only upon "a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility."[42] By contrast, section 215 contains no limiting language regarding who can be served with an order to produce "any tangible things." Thus, a FISA production order potentially could be served upon any entity with access to the information sought by the government. Such mechanisms are, however, subject to the relevant jurisdictions of the relevant courts.

3.54 Third, section 215 modified the relevance standard for an order related to the production of records (or, now, "any tangible items") and expanded the circumstances justifying such an order. Previously, the U.S. government was required to specify that there were "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[43] Now, under section 215, the government need only specify "that the records concerned are sought for an authorized investigation ... to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[44]

---

40 *See* Pub. L. No. 105-272, tit. VI, § 602, 112 Stat. 2411 (1998) (formerly codified at 50 U.S.C. § 1862(a) (2000)) (emphasis added).

41 50 U.S.C. § 1861(a)(1) (emphasis added).

42 Pub. L. No. 105-272, tit. VI, § 602, 112 Stat. 2411 (1998) (formerly codified at 50 U.S.C. § 1862(a) (2000)).

43 *Id.* (formerly codified at 50 U.S.C. § 1862(b)(2)(B)). A "foreign power" includes: a foreign government; an entity controlled by a foreign government; a group engaged in international terrorism; or a foreign-based political organization. *See* 50 U.S.C. § 1801(a). An "agent of a foreign power" includes: a non-U.S. person who acts as an officer or employee of a foreign power; a non-U.S. person who acts on behalf of a foreign power which engages in clandestine intelligence activities against the interests of the U.S.; any person who knowingly engages in clandestine intelligence gathering activities against the interests of the U.S. for or on behalf of a foreign power, which may involve a violation of federal criminal law; any person who knowingly engages in sabotage or international terrorism for or on behalf of a foreign power; or any person who knowingly assumes a false identity in the United States for or on behalf of a foreign power. 50 U.S.C. § 1801(b).

44 50 U.S.C. § 1861(b)(2). "Foreign intelligence information" includes information relating to, and if concerning a U.S. person necessary to, the country's ability to protect against: attack or hostile acts of a foreign power; sabotage or international terrorism by a foreign power or its agent; or clandestine

The government no longer must make any attestation about "the person to whom the records pertain." Accordingly, under section 215, a FISA order may require the production of "tangible things" pertaining to anyone, provided that the information sought is related to an investigation to obtain foreign intelligence information not concerning a United States person, or to protect against international terrorism or clandestine intelligence activities.[45]

3.55 Section 215 has created considerable controversy in the U.S. For instance, we understand that over 300 U.S. municipalities and 4 states have criticized that section.

3.56 Unlike grand jury subpoenas, section 215 applies beyond criminal investigations to include investigations "to obtain foreign intelligence information ... or to *protect against* international terrorism or clandestine intelligence activities."[46]

3.57 Section 215 also provides greater discretion to law enforcement than a grand jury subpoena: whereas a grand jury subpoena is subject to judicial review of its scope and reasonableness, the court's review of a Section 215 application is limited to ensuring the records sought are related to an authorized investigation.

3.58 A person served with a *Patriot Act* order is not permitted to disclose the fact of the order to anyone other than those persons necessary to produce the items sought.

3.59 The U.S. Justice Department has publicly taken the position that section 215 allows order recipients to move to quash; *Muslim Community Association v. Ashcroft*, No. 2:03-cv-72913-DPH (E.D. Mich.). Here is an excerpt from its submissions; "And nothing in Section 215 purports to block plaintiffs from raising -- prior to making production -- any constitutional or other objections to the FIS Court's order, and nothing relieves the FIS Court of its responsibility to resolve those objections." (Page 1) "Plaintiffs thus can face no threat of sanctions

---

intelligence activities by a foreign power or its agent. It also includes information relating to, and if concerning a U.S. person necessary to, the national security of the U.S. or the conduct of the foreign affairs of the U.S. 50 U.S.C. § 1801(e).

"International terrorism" includes activities that: (a) involve violent acts or acts dangerous to human life that are a violation of state or federal law; (b) appear intended to coerce a population, influence the policy of the government by intimidation or coercion, or involve assassination or kidnapping; and (c) occur outside the U.S. or transcend national boundaries. 50 U.S.C. § 1801(c).

"Clandestine intelligence activities" is not a defined term under the statute.

45 The FISA court's review of a Section 215 application is limited to the nature of the investigation, rather than the subject of the records. Specifically, under the terms of the statute, a judge is to review the Section 215 application to ensure: (a) that the records are sought for an authorized investigation to obtain foreign intelligence information not concerning a U.S. person, or to protect against international terrorism or clandestine intelligence activities; (b) that the investigation is conducted under guidelines approved by the Attorney General under Executive Order 12333 or a successor order; and (c) that the investigation is not being conducted of a U.S. person solely upon the basis of protected First Amendment activities. *See* 50 U.S.C. § 1861(b)(2).

46 50 U.S.C. § 1861(a)(1) (emphasis added).

under Section 215 without, first, being served with a Section 215 order and given an opportunity to move the FIS Court to quash the order." (Page 4) "Nothing in Section 215 authorizes the FIS Court to close the courthouse door to appropriate pre-production motions (e.g., a motion to quash) . . . ." (Page 13) "However, when Congress conferred jurisdiction on the court to issue an order requiring production of documents, it explicitly authorized that court to determine whether the order complies with the statute and implicitly authorized that court to ensure that its order is constitutional."

3.60 Section 218 of the *Patriot Act* encourages an integrated antiterrorism campaign by allowing the use of FISA whenever "a significant purpose" of the investigation is foreign intelligence. The Province does not see that section as creating a potential risk of access to government information in Canada.

3.61 Section 505 of the *Patriot Act* expands the authority of U.S. law enforcement authorities to order certain institutions, namely banks, credit reporting agencies, and internet service providers, to provide customer information. The Province does not see that section as creating a potential risk of access to government information in Canada.

Service of a Patriot Act Order

It is unlikely that the U.S. court would assume direct jurisdiction over a Canadian company with US connections operating in Canada, and it is further unlikely that a Canadian company would even be served with a Patriot Act order without the consent of the Canadian Government.

3.62 As outlined in paragraphs 2.26 to 2.29 above, it is unlikely that a U.S. court, including the FIS court, would have the requisite constitutional jurisdiction to issue an order for the production of records directly to a Canadian company with US connections, operating solely in Canada.[47]

3.63 To repeat the law outlined above, it is well-settled in the United States that a U.S. court's ability to exercise civil and criminal authority over an entity — including for purposes of compelling production of materials — extends only as far as its constitutional jurisdiction. Under U.S. law, foreign entities are subject to a grand jury subpoena to the extent that they would otherwise be subject to the jurisdiction of the U.S. court.[48]

---

47 *See supra* note 23.

48 These same jurisdictional constraints apply to the "gag" provision of Section 215, which states that "[n]o person shall disclose to any other person . . . that the [FBI] has sought or obtained tangible things," 50 U.S.C. § 1861(d), carrying an implicit threat of a contempt sanction for failure to comply. *See* 18 U.S.C. § 401(3). Neither this provision nor its enforcement mechanism extend beyond the jurisdictional limits of the issuing court.

3.64 In any given case, the questions of whether a Canadian company, under U.S. law, has the requisite "minimum contacts" with the U.S. jurisdiction, and whether the U.S. court would determine that to take jurisdiction would not "offend traditional notions of fair play and substantial justice", would depend on the particular facts of the case.

3.65 Again to reiterate, the simple fact of the corporate relationship between the Canadian company and its US parent is likely not enough to satisfy the "minimum contacts" test to provide U.S. jurisdiction over the Canadian or B.C. company.

3.66 Another factor that would play into a decision by the U.S. authorities to seek an order directly against a Canadian company is that fact that service (as opposed to issuance) of a subpoena *duces tecum* upon such a corporation within Canadian territory may only be effected with the consent of the Canadian government.[49]

3.67 With respect to companies contracting with the British Columbia government, if those companies do not have significant business activities in the U.S., and if they are sufficiently independent from their U.S. corporate affiliates in the sense that the U.S. corporate affiliate does not carry on business in the U.S. on behalf of its British Columbia affiliate, the U.S. court will not have personal jurisdiction over the British Columbia company for the purposes of exercising a power to compel the production of records to the U.S. authorities.

3.68 In the likely circumstances that the U.S. court would have no personal jurisdiction over British Columbia companies, the most likely scenario in terms of the issuance of an order under the *Patriot Act* (assuming that the U.S. would opt to proceed under the *Patriot Act* at all) would be for the FIS court to issue the order to the U.S. affiliate of the British Columbia company. The U.S. company would then be responsible for obtaining the information from the British Columbia company.

3.69 The risk that an individual, including a U.S. citizen or resident working for a company in Canada, would receive a *Patriot Act* order for the compulsion of documents belonging to their Canadian employer is very small.[50]

---

[49] Indeed, the act of serving compulsory process upon a foreign entity overseas "constitutes an exercise of one nation's sovereignty within the territory of another sovereign," which may violate principles of international law. *Compagnie de Saint-Gobain-Pont-A-Mousson*, 636 F.2d at 1313; *see also Ings v Ferguson*, 282 F.2d 149, 151 (2d Cir. 1960) ("[S]ervice of a United States District Court subpoena by a United States Marshal upon a Montreal branch of a Canadian bank would not be enforceable. However, amongst civilized nations, between which international comity exists, procedures have long been established whereby the requests of litigants in other countries seeking testimony and records are honored."); *United States v. Theresius Filippi*, 918 F.2d 244, 246 n.2 (1st Cir. 1990) ("The United States has no subpoena power over a foreign national in a foreign country.").

[50] *In re Sealed Case* 266 U.S. App. D.C. 30, *supra* (text accompanying notes 2-4)

3.70 In such an event, the Province believes that various types of mitigation strategies can be implemented to limit the likelihood of a finding by a FISA court that a U.S. company had access to, or control of, information held by a Canadian affiliate, therefore precluding any legal obligation (under U.S. law) to produce such records. Further, by employing appropriate and effective mitigation strategies, the government would create significant corporate, financial, technological and (provincial) legal impediments to the production of that information by the Canadian company.

4. The Risk of Access to Canadian Information under the Patriot Act

The Commissioner has stated as follows: "Returning to my theme, it is crucial after 9/11 that decision-makers not abdicate their responsibility to, as disinterestedly as possible, do three things. First, our elected representatives – they work for us, after all – must focus on real risk. Second, they must at all times act on the knowledge that risk can never be eliminated. Third, they must act on the principle that pandering to fear, much less creating the conditions for it to flourish, are not acceptable in a free and democratic society". [51]

Public bodies need to make decisions concerning security with the information they have concerning the magnitude of the risk, knowing full well that perfect security can never be attained.

The Province believes that the Patriot Act poses only a small incremental risk in relation to information held in Canada and B.C.

4.01 We must be dispassionate and reasoned in dealing with the risk of access to Canadian information under the *Patriot Act* and base our decisions on an objective analysis of the facts and U.S. law. As such, we must resist pandering to unfounded fear.

The Jaffer Opinion

The Jaffer Opinion does not quantify the risk of FBI access to information in the hands of a Canadian or B.C. company. Nor does it consider whether that risk can be mitigated.

4.02 The Commissioner has attached the opinion of Jameel Jaffer to his Request for Submissions (the "Jaffer Opinion"). That opinion dealt with the potential for a section 215 order under the U.S.A. Patriot Act. However, the Province notes that the Jaffer Opinion makes no attempt to quantify the level of risk of FBI access to information in the hands of a Canadian or B.C. company. The Province does so in these submissions. Nor does the Jaffer opinion offer a view as to whether, to the extent that there is risk, such a risk can be mitigated. The Province will make submissions on that issue as well. The Province submits that those two issues are significant to an analysis of the issues under review.

4.03 Moreover, there is no reference in the Jaffer Opinion of the extent to which lawful cross-border arrangements pre-dating passage of the *Patriot Act* are relevant to

---

51 "Identity, Privacy & Security—Can Technology Really Reconcile Them?"

any determination as to what, if any, incremental privacy risk is posed by the *Patriot Act*. For instance, as mentioned, prior to the passage of the *Patriot Act* there were other existing mechanisms for U.S. law enforcement agencies to potentially gain access to information held in Canada, i.e. grand jury subpoenas, requests under the *Mutual Legal Assistance Treaty* and legally sanctioned information sharing arrangements with Canadian law enforcement agencies.

It is unlikely that the U.S. will demand the production of personal information held in Canada without Canada's concurrence.

4.04 We believe that it is unlikely that the U.S. will attempt to demand production of information held in Canada without Canada's assistance and/or concurrence because: (1) foreign governments generally object when the U.S. seeks to extend its laws extra-territorially (i.e., "Bank of Nova Scotia subpoenas"); (2) the US knows this and has responded by entering into agreements like the MLAT, as well as the U.S. Department of Justice now requiring its prosecutors to receive the approval of the OIA before subpoenaing records held abroad; and (3) it is reasonably anticipated that the caution the U.S. has exercised with respect to the extraterritorial application of already existing processes will be even greater with respect to the *Patriot Act* due to the domestic controversy it has generated.

4.05 Based on the experience with "Bank of Nova Scotia" subpoenas, it is anticipated that the ability of U.S. federal prosecutors' to utilize the *Patriot Act* will be governed by the same or similar U.S. Attorneys' Manual rules that govern the issuance and enforcement of Bank of Nova Scotia subpoenas.[52]

4.06 Among the considerations to be taken into account by the OIA in determining whether a subpoena with extra-territorial application should be authorized is the availability of alternative methods, such as the use of a mutual assistance treaty.[53] Indeed, the controversy surrounding *Bank of Nova Scotia* subpoenas was one of the primary catalysts for the MLAT between the U.S. and Canada. As the U.S. Technical Analysis explains, "Canada viewed these subpoenas as intrusions on its sovereignty but recognized that the United States had no alternative in those cases where Canada was prevented by its law from assisting the United States".[54]

4.07 Given the continuing use of the U.S.-Canada MLAT as an avenue of first resort, the availability of grand jury subpoenas in the U.S., as well as existing legally authorized information sharing mechanisms between Canadian and U.S. law enforcement agencies that do not require court orders to share information, we

---

52 See footnote 99 of Thomas G. Snow, *The Investigation and Prosecution of White Collar Crime: International Challenges and the Legal Tools Available to Address Them*, 11 WM. & MARY BILL RTS. J. 209, 233 (2002).

53 *Supra*, note 27.

54 Senate Report, at 3.

believe that it is reasonable to conclude that U.S. authorities will view the *Patriot Act* as a less desirable means of seeking records held abroad.

4.08 The Province therefore believes that the *Patriot Act* poses only a small incremental risk in relation to personal information held in British Columbia. Of course we cannot say that that would never happen. However, public bodies need to make decisions concerning security with the information they have concerning the magnitude of a risk, knowing full well that perfection is not a standard that is required or can ever be reached. Based on the information available to us, the Province believes that there is no reason to think that the risk of access to Canadian information under the *Patriot Act* is anything other than minimal, especially in the event that appropriate mitigation strategies are implemented.

4.09 To the extent that a request for records relates to a potential criminal offense, the U.S. authorities are obligated first to seek them through the MLAT. Further, in the event that the terms of the MLAT were unavailable (i.e., because the records were not sought for an investigation of potential criminal conduct), and the records nevertheless were necessary for clandestine intelligence or to thwart a terrorist act, it is likely that U.S. and Canadian authorities would seek alternative means to cooperate (i.e., means outside of the *Patriot* Act). In light of official U.S. Department of Justice guidance to prosecutors about heeding the importance of allied relationships,[55] the Province believes U.S. authorities would hesitate to risk the close strategic relationship with Canada — including in particular on law enforcement and intelligence issues — by trying to compel a U.S. company or a U.S. citizen living in Canada to procure government information held in Canada.

4.10 The provisions of the *Patriot Act* must be viewed in the context of broader law enforcement and discovery mechanisms available to the U.S. government before the passage of that Act. There are a number of reasons that U.S. authorities would prefer the MLAT as a mechanism to obtain records located in Canada, and in all events, U.S. authorities must first seek to obtain such data through the MLAT, where the treaty applies to that information — and, if the MLAT terms themselves prove unavailing, pursue options for a compromise arrangement — before turning to other domestic investigative tools.[56] In the event that assistance is unavailable under the MLAT or a compromise arrangement, grand jury subpoenas are a proven method and, depending on the circumstances, may be a more likely alternative than a section 215 order. Thus, while section 215 on its face appears to expand U.S. law enforcement authority, and while we cannot rule out the possibility that U.S. authorities could at some point utilize this authority to compel a U.S. company to produce government data held in Canada where that company has control of, or the right to access, that data (e.g., if assistance is unavailable under the MLAT), the Province believes that such a result is unlikely.

---

55 *See supra* note 27.

56 *See* Technical Analysis, at 13 (Article IV of the Treaty provides that "a party needing documents, records, or articles located in the territory of the other and not available under any cooperative agreement or arrangement must use the Treaty to obtain them.").

The Province believes that U.S. authorities will likely view the *Patriot Act* as a less desirable means of seeking access to records held abroad.

4.11 As noted, the evidence is that section 215 of the *Patriot Act* was not used in the first two years after proclamation. See the attached Department of Justice memo dated May 19, 2004, attached as Appendix "D". While we do not know whether any s. 215 orders have been issued since that time, that does not discount the fact that we do know that no such orders were issued within the first two years. Again, we need to objectively consider the facts, and not pander to fear, when dealing with issues of security. Before it was amended by section 215, FISA section 501 was used fewer than five times.[57]

4.12 Of relevance to the section 30 analysis is that there is a sunset clause of December 31, 2005 currently in place for s. 215 of the Patriot Act. Thus, there is a distinct possibility that the privacy concerns arising out the potential application of s. 215 may be short-term. While U.S. President Bush has stated publicly his position that the provisions covered by the sunset clause, including s. 215, ought to be renewed, the present state of the law in the U.S. is that section 215 is due to expire in approximately 17 months, after the upcoming U.S. federal election. The Province submits that it would be inappropriate to dictate British Columbia policy on the assumption that this infrequently used section will be renewed.

There should be a national discussion about privacy.

4.13 The Province will continue to consult with the Government of Canada in order to obtain their views on the threat of the potential use of the *Patriot Act* with respect to Canadian information and to ensure that Canada affirms the international obligations of the U.S. with respect to information sharing, and receives appropriate assurances that existing established mechanisms will be used when Canadian information is required for security or law enforcement purposes.

Summary

4.14 The Province submits that the following considerations support a finding that the *Patriot Act* creates only a small incremental risk of disclosure of personal information to U.S. law enforcement authorities;

---

[57] Charles Doyle, *The USA PATRIOT Act: A Legal Analysis*, CRS Report for Congress, RL31377 (April 15, 2002) at n.41, *available at* http://www.fas.org/irp/crs/RL31377.pdf (last visited July 18, 2004) (citing the U.S. Department of Justice's Patriot Act proposal, which was printed as an appendix in *Administration's Draft Anti-Terrorism Act of 21001, Hearing before the House Comm. on the Judiciary*, 107th Cong., 1st Sess. 54 (2001). CRS 'is the public policy research arm of the United States Congress'. *See* http://www.loc.gov/crsinfo/whatscrs.html#about (last visited July 19, 2004).

- There exist other lawful personal information sharing processes between law enforcement agencies in Canada and the United States that will likely be utilized prior to resorting to the *Patriot Act*;

- For instance, the MLAT will continue to be the avenue of first resort for U.S. law enforcement authorities in relation to information found in Canada that relates to suspected criminal activities;

- Prior to the enactment of the *Patriot Act*, grand jury subpoenas were capable of compelling the production of information held in Canada where a U.S. company had control of, and access to, data of a Canadian affiliate (though the usage of such subpoenas has diminished since the MLAT was signed). As such, Canadian information was potentially subject to disclosure to U.S. authorities prior to the passage of the *Patriot Act*;

- The perception that unilateral U.S. demands for records held abroad are an improper assertion of extraterritorial power by the US. The existing U.S. process calls for OIA to vet requests to seek the production of information held abroad . The U.S. executive branch, for instance, discourages the use of mandatory order to obtain records held abroad; and

- Mitigation strategies are available to ensure that a U.S. company does not have access to, or control of, public body supplied personal information that is held by a Canadian affiliate. Such measures can effectively minimize the risk of access to Canadian information under the *Patriot Act*.

4.15 Given the small incremental risk to Canadian information posed by the *Patriot Act*, the Province believes that disclosing sensitive personal information to a B.C. or Canadian company with U.S. connections in the course of public body outsourcing would not contravene the FOIPP Act provided that a public body:

- Employs mitigation strategies to ensure that the B.C. or Canadian company's U.S. affiliate does not have access to, or control of, such personal information and that such mitigation strategies are commensurate with the sensitivity of the personal information in question; and

- Ensures that there are contractual provisions in place dealing with both privacy and security issues and that such provisions are commensurate with the sensitivity of the personal information in question.

4.16 With respect to personal information sent to the U.S. on a temporary or permanent basis, the risk of access to such information by the U.S. Federal Bureau of Investigation under the *Patriot Act* is likely greater because government mitigation strategies will have less impact in such situations. However, public bodies can take steps to minimize the extent to which any sensitive personal

information is sent to the U.S. on a temporary or permanent basis. For its part, Government will not send sensitive personal information to the US either on a temporary or permanent basis.

4.17 With respect to non-sensitive information, because of the small incremental nature of the risk of access under the *Patriot Act*, there may be cases where mitigation strategies to deal with that risk are not necessary. Rather, in such cases the addition of the customary contractual language dealing with privacy and security issues may meet the requirements of section 30 of the FOIPP Act. The Province will assess each of these situations individually.

5. NAFTA, WTO and AIT

In assessing the security arrangements that a "fair and rational" person would expect to be made, one should also consider the impact of trade and investment obligations arising under the North American Free Trade Agreement ("NAFTA"), the agreements of the World Trade Organization ("WTO"), and other international trade and investment agreements, as well as the inter-provincial Agreement on Internal Trade ("AIT").[58]

5.01 The Province submits that a fair and rational person would not consider it reasonable to expect public bodies to exclude companies with U.S. connections from bidding on contracts where to do so would violate international treaty obligations.

5.02 The Government of Canada has agreed, pursuant to the terms of international trade and investment agreements, to ensure that the governments of British Columbia and other provinces and territories comply with the obligations arising under the above-mentioned international trade and investment agreements.

5.03 NAFTA Article 105 provides that Canada is required to "ensure that all necessary measures are taken in order to give effect to the [NAFTA] provisions..., including their observance ... by state and provincial governments".

5.04 Article I:3 of the WTO's *General Agreement on Trade in Services* ("GATS") requires Canada to take "such reasonable measures as may be available to it to ensure their observance by regional and local governments and authorities". Canada is bound by an almost identical obligation regarding provincial measures affecting trade in goods pursuant to Article XXIV:12 of the WTO's *General Agreement on Tariffs and Trade 1994* ("GATT 1994").

5.05 Any implementation of an outsourcing arrangement that violates Canada's commitments under NAFTA or the WTO can be subject to challenge by other countries pursuant to government-to-government dispute resolution mechanisms established under these agreements. Canada's failure to amend or remove measures determined to be inconsistent with its obligations under these agreements will likely result in retaliatory actions from its trading partners. Furthermore, under NAFTA Chapter 11 and other investment agreements, private investors may sue Canada for loss or damages incurred as a result of the implementation of provincial measures that violate Canada's investment obligations.

---

[58] As a Party to the AIT, the Province of British Columbia is subject to numerous obligations regarding goods, services, investments, and government procurement.

5.06 There are a number of NAFTA and WTO obligations which may impact the design and implementation of an outsourcing arrangement by the government. Examples of significant commitments in this regard include the following:

(a) to treat NAFTA investors no less favourably than Canadian investors (national treatment) or investors from non-NAFTA countries (most-favoured-nation treatment) (NAFTA Articles 1102 and 1103);

(b) to accord to the investments of NAFTA investors fair and equitable treatment and full protection and security (NAFTA Article 1105);

(c) to refrain from use of performance requirements, for example, measures imposed on investors encouraging exports or favouring the domestic sourcing of goods or services (NAFTA Article 1106 and the WTO's *Agreement on Trade-Related Investment Measures*);

(d) to compensate NAFTA investors for expropriation, or measures tantamount to expropriation, of their investments (NAFTA Article 1110);

(e) to accord national treatment and most-favoured-nation ("MFN") treatment to services and service suppliers from NAFTA and WTO member countries (this includes financial services) (NAFTA Chapters 12 and 14, GATS);

(f) to provide market access to services and service suppliers from NAFTA and WTO member countries and to refrain from imposing limitations on the number of service suppliers (NAFTA and GATS Article VIII); and

(g) to accord national treatment and MFN treatment to the goods of NAFTA and WTO member countries (NAFTA and GATT 1994).

5.07 NAFTA and the agreements of the WTO also contain reservations, exceptions and qualifications regarding certain of these obligations. Their application will depend on the particular project and the circumstance surrounding its implementation. Such exceptions include the following:

(a) procurement of goods and services by government is exempt from the application of certain obligations

(furthermore, at the present time, provincial governments and entities are not subject to NAFTA and WTO government procurement obligations);

(b) certain NAFTA investment and services obligations do not apply to measures regarding public law enforcement, correctional services, and certain social services established or maintained for a public purpose, including income security or insurance, social security or insurance, social welfare, public education, public training, health and child care;

(c) certain NAFTA investment and services obligations do not apply to measures regarding rights or preferences accorded to aboriginal peoples or socially or economically disadvantaged minorities;

(d) certain NAFTA investment and services obligations do not apply to non-conforming provincial measures that existed on January 1, 1994;

(e) Canada's GATS market access and national treatment obligations apply only to those service sectors identified in Canada's Schedule of Commitments; and

(f) Canada's services commitments at the WTO are subject to certain exceptions, including those for measures necessary to protect human, animal or plant life or health, measures necessary to protect public morals or maintain public order, and measures to ensure compliance with laws not inconsistent with GATS (provided that they do not constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on international trade).

5.08 In order to determine whether any of these WTO or NAFTA obligations apply, and whether any exceptions may be available, it will be necessary to carefully review a proposed outsourcing initiative and assess it against these commitments.

6. Other Security Risks

Any reasonable security analysis should not consider in isolation any incremental risk posed by the Patriot Act, but should consider what is "reasonable" in light of all potential risks to the unauthorized disclosure of personal information.

6.01 It is generally accepted that the most significant threat to an organization's security is from within, namely, the risk that an employee will inappropriately disclose information, whether intentionally or inadvertently. Many security incidents result because someone within an organization that has access to data either intentionally or inadvertently compromises the security of that data. Such a risk will exist regardless of whether the data is managed by government or by private sector firms. For instance, much has been written about the tactics of "social engineers" (hackers) to obtain access to confidential data in the hands of both public and private organizations.

6.02 The Province submits that any s. 30 analysis should not consider in isolation any incremental risk posed by the *Patriot Act*, but should consider what is "reasonable" in light of all the potential risks to the unauthorized disclosure of personal information, including human error and malfeasance (e.g. leaks and "hackers"), which, the Province believes, is a far greater security risk than is potential access under the *Patriot Act*.

6.03 For instance, it may be unreasonable to devote considerable resources to a very small security risk such as *the Patriot Act*, when doing so means that other more serious risks may not be adequately dealt with. Also of relevance to the section 30 analysis is the extent to which outsourcing arrangements may provide improved security against such risks. For instance, there may be some areas where large companies with U.S. connections, because of their infrastructure and expertise, as well as their ability to access top international practices and their experience in managing large databases, may be able to make security arrangements in some areas that are superior to the arrangements that can be made by a competitor without U.S. connections. If that is the case, it may well be that the minimal risk posed by the *Patriot Act* in the event that a company with U.S. connections is chosen to manage government information could be more than offset by the superior security arrangements that could be implemented to avert other more serious security risks.

7. Privacy Protection Measures

To further reduce any possible risk of disclosure of British Columbians' personal information under the Patriot Act, Government will implement enhanced privacy protection measures in its arrangements with service providers.

There are four key objectives with respect to the protection of personal information that should be considered in any outsourcing arrangement where U.S. companies are involved. Mitigation strategies, summarized in Appendix "E" are directed at meeting one or more of these objectives:

- ***Measures to Limit the Application of the Patriot Act – so that the Patriot Act does not apply;***
- ***Restrict Ability of U.S. Company to Compel Disclosure;***
- ***Advance Notice of Potential Disclosure; and***
- ***Incentives to Prevent Disclosure.***

Measures to Limit the Application of the Patriot Act.

7.01 As is the case with grand jury subpoenas, we believe that a U.S. company served with a section 215 order would likely be obligated to produce any documents that it had the right to access or control.[59]

7.02 As such, given the principles articulated in cases involving the extraterritorial application of subpoenas, we think it unlikely that a U.S. company could be compelled to produce records over which the company has no control nor any right or ability to access, even in the face of a Section 215 order.[60] Indeed, if a Section 215 order were served on the U.S. company, the risk of disclosure of the records would appear to be minimal or nonexistent if, as a practical matter, the U.S. company had no ability to comply with the demand.

7.03 The Jaffer Opinion, obtained by the BCGEU states that "whether a United States corporation would be required to produce the records of its Canadian affiliate in any particular case would likely turn on the specific legal relationship between the two corporations and on whether the United States corporation could access and obtain the records at issue". The Province agrees with that statement.

---

[59] *See In re Marc Rich & Co., A.G.*, 707 F.2d 663, 667 (2d Cir. 1983), *cert denied*, 463 U.S. 1215 (1983).

[60] The term "control" includes not only physical possession and the legal right to obtain the documents requested upon demand, but also access to the documents and the ability to obtain them for a company's usual business.

7.04 We believe that public bodies can structure their outsourcing agreements to make clear that a U.S. company affiliated with the Canadian or B.C. service provider does not have access to, or control of, personal information supplied by the public body. If that is done, we believe that a U.S. company would not be required to produce such records in the event it was served with an order under the *Patriot Act*.

Restrict Ability of U.S. Company to Compel Disclosure

7.05 An important objective should be to limit the ability of a U.S. company to compel disclosure of information by its Canadian affiliate (even where it does not have direct access to the personal information).

Advance Notice of Potential Disclosure

7.06 Advance notice of a potential disclosure allows all of the parties involved to take additional steps to ensure that personal information does not, in fact, get disclosed. The effectiveness of measures to prevent disclosure is therefore enhanced where the Province has advance notice of a potential disclosure of personal information under the *Patriot Act*. While the U.S. company receiving an order under section 215 of the Patriot Act would need to comply with the secrecy requirements of that Act, their Canadian or British Columbia affiliate would not.

7.07 In addition, the imposition of advance notice requirements in contracts, along with extensive audit requirements, will be at odds with the secrecy that is such a large part of the *Patriot Act*. The Province believes that such measures will made a *Patriot Act* order an even less attractive option for U.S. authorities.

Incentives to Prevent Disclosure

7.08 The Province will align the interests of the service provider with the interests of the Province. This is achieved through the implementation of incentives for the U.S. company and its Canadian affiliate to comply with the non-disclosure requirements of the outsourcing arrangement. It is also achieved through the implementation of consequences where the non-disclosure obligations are breached by the U.S. company or its Canadian affiliate.

The Province has developed a set of privacy protection measures that will be deployed on a case by case basis to each of the ASD initiatives to meet the above objectives. Those measures will be implemented on the legislative foundation of the FOIPP Act that will include amendments that government will be proposing.

7.09 Those privacy protection measures fall into four general categories as follows:

(a) *Technology and Business Processes*: Technology and business process strategies focus on limiting access to personal information solely to authorized people in British Columbia and otherwise ensuring that "leading practices" are used to secure personal information. This includes such things as the limitation of access through physical, logical and remote security, restrictions on data mobility, and audits to monitor use of personal information, etc...;

(b) *Employee Strategies*: Employees are the people that have access to personal information on a daily basis and who have the power to make choices around disclosure. Strategies such as whistle blower protection, privacy training, confidentiality agreements, and residence/citizenship requirements are examples of employee strategies;

(c) *Contractual Measures*: Protection of privacy will be built into the outsourcing contracts with severe penalties for non-compliance, including such things as termination of contract, liquidated damages, and step-in rights; and

(d) *Corporate Structures*: There are a number of corporate structuring approaches that can be implemented to limit or restrict the ability of a U.S. based parent company from directing its Canadian subsidiary to disclose personal information, such as the establishment of trust structures and requiring all Canadian directors on Canadian based subsidiaries.

7.10 The mitigation strategies summarized in Appendix "E" of these submissions are directed at meeting one or more of those objectives. Determining which of those mitigation strategies should be implemented in a given case depends on the sensitivity of the data in question.

Appendices E, F and G of this document provide more examples of effective mitigation strategies, including examples of the comprehensive protection that are being considered in connection with government's arrangement with Maximus Inc. in the Health Benefits Operations Project.

7.11 The Province has selected Maximus Inc. to work with the Province on developing a new service delivery model for the Medical Services Plan and Pharmacare. Appendices "F" and "G" outline mitigation strategies the parties are considering in dealing with the *Patriot Act* issue.

7.12 The Health Benefit Operations Project mitigation solutions found at Appendix "G", and especially the Trust Structure, have been developed specifically for that project and would not necessarily be appropriate or possible for some of the other ASD projects. As mentioned, there is no one size fits all solution that can be applied across all projects.

7.13 The Province also refers you to Appendix "H" which further outlines the enhanced privacy protection measures which are proposed for the Health Benefit Operations Project. Privacy will not only continue to be protected, but that protection will be greatly enhanced.

8. Legislative Options

In order to ensure the highest possible protection against the risk of access to government information under the Patriot Act, government will propose amendments to make the strongest privacy legislation in Canada even stronger.

8.01 Government will propose the following:

- Amending protection of privacy provisions in the FOIPP Act to apply privacy standards directly to service providers in relation to personal information supplied to them by public bodies, and to expressly prohibit service providers from disclosing such personal information unless permitted by the FOIPP Act;

- Amending the FOIPP Act to require that a person having custody or control of personal information provided by a public body provide notice to government in the event that the person receives an order, subpoena, demand or request from a foreign court or body for the production of that information, or receives a request to disclose such information to an affiliated company for the purpose of complying with such an order, subpoena, demand or request;

- Including "whistle blower protection" in legislation to protect persons who provide such notice; and

- Creating offences in the event that someone violates such requirements.

9. Scope of the Patriot Act Issue

The present issue is not just an issue for governments in Canada, it is also an issue for the private sector.

9.01 It is worth noting that, to the extent that there is a potential risk of access to Canadian information under the *Patriot Act*, that risk applies to a wide variety of information across Canada, not just government information. Namely, that risk applies to information held by the private sector, not just to information held by public bodies. As such, the present issue is not just an issue for governments in Canada, it is also an issue for the private sector.

9.02 The Province notes that the potential risk of access to personal information held in the private sector under the *Patriot Act* will be an issue regardless of the outcome of this review. Such a risk will exist with respect to personal information held by Canadian or British Columbia corporations having U.S. connections, including the following types of personal information:

- Personal information collected by Canadian companies with U.S. connections through the issuance of customer reward cards. Personal information is collected by those companies at the time a customer applies for such cards. Such information is often collected and used for marketing purposes;

- Personal information collected by Canadian airlines through the issuance of frequent flier cards. Canadian airlines involved in such plans may exchange customer information with foreign airlines who also participate in those plans;

- Personal information collected by Canadian or British Columbian unions that have connections with U.S. unions. Such personal information will include union membership lists;

- Personal health information held by pharmacies (e.g. Walmart), insurers and medical service providers with U.S. connections;

- Credit card information held by companies with U.S. connections (e.g. American Express);

- Employee and customer information held by Canadian retail companies with U.S. connections; and

- Personal information held by Canadian internet service providers with U.S. connections. Such information will be found in personal e-mails that are kept on the servers of those internet service providers.

9.03 No matter what you decide in this forum, all Canadians will continue to be faced with the reality that companies with U.S. connections will continue to operate in Canada and will continue to collect and use personal information of Canadian residents, regardless of any government outsourcing. As such, the risk of *Patriot Act* access will need to be addressed by all jurisdictions across Canada, as well as in other countries, regardless of the impact of this review on public bodies in British Columbia.

9.04 Having said that, this has been a valuable process for the province to undertake, and the assessment that has resulted helps guide our government in taking the appropriate measures to continue to ensure that the personal information of British Columbians is protected.

10. Conclusion

10.01 The *Patriot Act* issues identified by you are only part of a much larger set of public policy issues for both the public and private sectors that involve balancing the interests of privacy with collective security in an interconnected global economy. The *Patriot Act* adds only a small incremental risk of disclosure of personal information to U.S. authorities.

10.02 British Columbia is committed to ensuring effective and efficient government services by taking advantage of alternative service delivery arrangements in conjunction with the private sector. At the same time, British Columbia is committed to privacy protection and is a leader in the privacy protection field.

10.03 To the extent that the application of the *Patriot Act* to alternative service delivery arrangements poses any additional privacy risks, these will be addressed in British Columbia by a combination of effective privacy protection strategies in arrangements with service providers, as well as the introduction of new legislative measures to strengthen privacy protection.

10.04 Government will also continue to work with the Government of Canada to ensure that Canada affirms the international obligations of the United States with respect to information sharing and receives appropriate assurances that existing established mechanisms for collecting information will be used when Canadian information is required for security or law enforcement purposes.

10.05 Thank you again for this timely and useful opportunity to review privacy protection issues and to reaffirm the Province's commitment to the protection of personal information of British Columbians. We look forward to reviewing your report and working with you to develop solutions to protect the privacy of British Columbians.

All of which is respectfully submitted,

Original signed by

The Honourable Geoff Plant
Attorney General of the Province
of British Columbia

Royal Canadian Mounted Police

Chapter 124

General Information

Background

The Royal Canadian Mounted Police was formed in 1873, under an Act of Parliament.

Responsibilities

The Royal Canadian Mounted Police enforces laws throughout Canada made by or under the authority of Parliament. Administration of justice within the provinces, including enforcement of the Criminal Code, is the responsibility of provincial governments. The RCMP has contract agreements with the three territories and all provinces, except Ontario and Quebec, to enforce criminal, territorial and provincial laws, pursuant to section 20 of the RCMP Act.

Legislation

- Criminal Code
- Most federal statutes
- Municipal bylaws under contract
- Provincial laws under contract
- Territorial laws under contract

Organization

The authority and accountability for executing the requirements of the RCMP Act rest with the Commissioner who reports to the Solicitor General of Canada. The Commissioner is supported by four regional Deputy Commissioners, and three Deputy Commissioner at the National Headquarters - responsible for Operations, Corporate Management and Comptrollership, and Strategic Direction - as well as an Assistant Commissioner responsible for National Police Services. The Commissioner also has a Chief Information Officer, a Chief Human Resources Officer and an Ethics Advisor who reports directly to him.

In addition, there are 14 divisional Commanding Officers and a Commanding Officer Depot Division (the RCMP training facilities in Regina, Saskatchewan) and 17 program directors at National Headquarters in Ottawa, Ontario.

The RCMP is divided into divisions, each division being roughly responsible for a province or territory. These divisions are alphabetically designated and each is further divided into subdivisions and detachments.

Specialized support is offered to the operational divisions by Air, Marine, Forensic Laboratory, and Identification Services. The RCMP Academy located in Regina, Saskatchewan, is responsible for recruit training. The RCMP Musical Ride is located in Ottawa and is administered by headquarters. Additionally, the RCMP is responsible for the administration of the Canadian Police College, located in Ottawa. The Canadian Police Information Center (CPIC), a computer-based police information system, is also based at and administered by RCMP Headquarters in Ottawa. The CPIC system is an advanced computerized information storage and retrieval facility, designed for the use of participating Canadian law enforcement agencies. The CPIC acts as a central repository of operational data that is contributed to and maintained by participating Canadian law enforcement agencies. RCMP records entered into the system are identified in their respective Bank of Personal Information. The participating Canadian law enforcement agencies are entirely responsible for the accuracy and immediacy of the data which they supply and maintain within the CPIC system. Records entered into the CPIC system by participating Canadian law enforcement agencies must be supported by documented reports held by the originator. The originating agency is the only one entitled or enabled to alter their records in the system.

Corporate Management and Comptrollership

The Corporate Management and Comptrollership service line objective is to provide expert functional policies, systems, services and advice to ensure the financial viability and stability of the RCMP, and the sound stewardship of all RCMP resources in the areas of financial management, asset and facility management, materiel, contracting, procurement and audit; and to ensure the strategic and practical national implementation of the Modern Comptrollership and the Financial Information Strategy, two major, long-term government initiatives focused on improved decision-making, organizational performance and accountability for results.

Strategic Direction

Strategic Direction service line objective is to develop and implement an overall RCMP policy framework for assessment of and participation in public policy debates affecting law enforcement, for capacity building in policy research and trend analysis and model building of various future scenarios affecting RCMP organizations and operations, for the development and

recommendation of various types of responses to future challenges involving change management analysis, for information exchanges and joint analysis of emerging trends and conditions, for policy and planning linkages, for critical on-going assessment of current internal policies and conditions and for media relations, promotion of the RCMP and of Canada, and the development of partnership contracts, including alternative funding with public and private partners.

Human Resources Activity

The Human Resources Activity encompasses the organization and management of the Department's human resources. It maintains an internal administrative policy function and service in relation to learning, staffing and personnel, health, materiel, language and organizational issues. These issues pertain to members of the RCMP as well as Public Service Employees employed by the organization. In addition, the Human resources Activity is responsible for the management of property, material, transport and food related services.

♦ Health Services

This program administers all health related assessment and treatment services to regular members of the RCMP and establishes health programs and standards for employment. It also manages research projects for the development of psychological services, fitness/ lifestyle programs as well as programs directed at promoting health and environmental safety. The Sub-Activity also maintains the medical records of members to ensure confidentiality.

♦ Learning and Development

The Employee Continuous Development Program fosters a continuous learning culture within the RCMP. It ensures RCMP employees have access to modern, cost effective learning/training opportunities consistent with the competencies required to deliver quality service to internal and external clients, to adapt and respond to diverse changing needs, and contribute to the evolution of the RCMP.

♦ Executive/Officer Development and Resourcing

This program provides a centralized staff support service to the Commissioner for the appointment, promotion, training, succession/ career planning of the Regular Member officers (Inspectors to Deputy Commissioners) and Civilian Members of officer equivalency.

♦ Human Resources (RCMP)

This program provides RCMP management with a number of diverse services to assist in management of the department's human resources. The Sub-Activity includes the following initiatives: Multiculturalism, Staffing & Personnel, Recruiting, Official Languages, Internal Affairs, Compensation, Classification, Honors and Recognition, Human Rights, employment equity and Conflict of Interest.

♦ Public Service Personnel

This program is responsible for the planning, design and implementation of an integrated human resource management program for Public Service Employees within the RCMP. This Sub-Activity is comprised of the following: Classification, Staffing, Staff Relations & Compensation, and Human Resources Planning and Development.

National Police Services Activity

The National Police Services (NPS) activity provides networked place information and information systems technologies and delivers investigative, scientific, technical and educational support serves to partners within the Canadian Police and justice environments.

♦ Canadian Police College

The Canadian Police College is an internationally recognized institution delivering advanced and specialized learning and training to Canadian and foreign police agencies. It is composed of the Police Executive Center, Police Science School, the CPC Library and the Business Services Branch.

♦ Criminal Intelligence Services Canada

This program is a national law enforcement community intelligence organization administered by the RCMP with a Central Bureau in Ottawa and nine provincial bureaux across Canada. The program, focusing on organized crime, gathers criminal intelligence and ensures that tactical intelligence is submitted through the provincial bureaux, where facilities for the collection, analysis and dissemination of criminal intelligence are provided, and are accessible to its members. The program oversees a computer system known as the Automated Criminal Intelligence Information Services (ACIIS), which is a repository for criminal intelligence information available to the intelligence community.

♦ Forensic Laboratory Services

This program provides scientific and technical assistance to the Canadian Criminal justice system. Physical evidence acquired during the course of investigations is examined by scientists, to provide information of evidential significance. Expert opinions based on scientific examinations are provided to aid investigations and as court evidence. The program maintains the national DNA Data Bank, which was established by the DNA Identification Act, on behalf of the Commissioner. This sub-activity also manages the

Canadian Police Research Centre which co-ordinates the development of scientific and technical research projects of a law enforcement nature. The program also provides a consultative service to other government departments, and an assistance role to other countries in relation to the transfer of expertise through training, analysis of exhibit materials and testimony within their judicial systems.

♦ The Office of the Chief Information Officer (O/CIO)

The IM/IT program is critical to the RCMP's mandated and strategic priority of ensuring safe homes and safe communities. The IM/IT function for the RCMP is governed by the Chief Information Officer (CIO), who is responsible for ensuring that client-centred services are developed and managed in the organization. The CIO's role is to create and maintain an organization that is business-driven, quality concious and carefully managed within its fiscal, human resource and IM/IT frameworks.

The corporate IM/IT program deals with the development and management of all aspects of information and computer technology which support the business requirements of the RCMP. This includes all hardware, software, application systems and programs, as well as all stored information. It also incorporates the convergence of telecommunications and radio communications' services that RCMP officers require across Canada. Finally, the IM/IT program supports the full life-cycle of both equipment and information and includes management practices that enable and aid in the legislated and sound usage of this information.

Information management provides for the maintenance, development and dissemination of applicable policies regarding recorded information, the management of archives, national forms policy and the editing, production and distribution of manuals, directives and bulletins. Information Technology includes all aspects of communication system standards and design, EDP application and operation of the central host mainframe and network systems, including the Canadian Police Information Centre (CPIC), the Canadian Police Information Retrieval System (PIRS), the *Police Reporting Occurrence System (PROS) and other operational, administrative and management support applications that are used on a national basis.

The objective is to provide a comprehensive national policy and program for the management of information resources, associated computer technologies and telecommunications infrastructure. Together these serve the needs of RCMP operational police officers, support and administrative staff, system users and others working in the law enforcement community.

*Note: The existing occurrence management system (PIRS) does not meet RCMP functionality or operational requirements. PROS will replace PIRS, redefined and rescoped to expedite the delivery of applications.

♦ Information & Identification Services

This program is dedicated to maintaining, managing and disseminating shared police information on behalf of the Canadian Law Enforcement Community and other accredited Canadian and international agencies. These support services include the automated fingerprint identification system (AFIS), the Canadian Firearms Registry (CFR), the Missing Children's Registry (MCR) and including a Forensic Identification and photographic service. The prime service line objective is to sustain a national leadership role in the development and implementation of the most efficient information technologies that support criminal justice initiatives in the prevention, detection and suppression of crime. This is accomplished through promoting national networking and cohesiveness within the field of Canadian police information systems and applied technologies.

♦ Professional Standards

This program supplies a centralized pool of legally trained RCMP members dedicated to providing representation and assistance to appropriate officers and members of the RCMP for formal discipline, discharge and demotion tribunals across the country.

♦ Technical Operations

Technical Operations (TO) primary focus is in the development of technical tools and systems to assist front line law enforcement personnel in the RCMP in their investigative duties. Research and technical support is conducted for lawful access techniques and systems, which includes CenCIS, covert entry, and computer search & seizure and forensic analysis. Further services are provided in the area Behavioral Science-based investigative and the response to counter criminal and terrorist acts primarily in the field of explosives agents. TO provides technical services in the area of physical security systems, including armored vehicles, for the protection of IPPs. The Departmental Security Program and the Air Services Program for the RCMP is also managed within TO. TO also assumes responsibility in providing Lead Agency and counter technical services in support of the Government Security Policy.

Operations Activity

The Operations Activity manages all planning and policy aspects of law enforcement programs in support of federal, provincial and municipal government requirements. Assistance and cooperation is provided to accredited police agencies as well as to the general

public. It is also the focal point, on a nation-wide basis, for the coordination and evaluation of criminal operations and criminal intelligence gathering. It encompasses the protective policing functions of the RCMP which includes providing security for designated government dignitaries; government property; internationally protected persons and their residences; and major events. It is responsible for coordinating security or VIP visits, conducting security inspections and surveys of physical installations and providing consultations for officials regarding security requirements.

♦ Community, Contract and Aboriginal Policing Services

This program initiates, develops and evaluates a practical and culturally sensitive policing program for aboriginal Canadians. Under contractual agreements, the Royal Canadian Mounted Police (RCMP) provides community-policing services to all provinces and territories except Ontario and Quebec. The RCMP provides policing services to municipalities that have negotiated an agreement with the Government of Canada, a limited number of airports and to a number of First Nation Communities through Tripartite Agreements. Municipal contracts are restricted to those provinces already policed by the RCMP.

♦ Criminal Intelligence

The mission of the Criminal Intelligence Directorate is to provide a national program for the management of the criminal information and intelligence which will permit the RCMP to detect and prevent crime having an organized, serious or national security dimension in Canada, or internationally as it affects Canada.

♦ Departmental Security

This program is responsible for developing, monitoring and coordinating the implementation of internal security policies relative to the security clearance of RCMP employees, properties and information systems.

Federal Services Directorate

Federal Services Directorate is currently made up of the following program areas.

♦ Customs & Excise

The Customs and Excise program enforces laws within Canada and along the Canadian/United States border, in conjunction with clients, partners and the community. These activities include: the international movement of dutiable, taxable, prohibited or controlled goods; the manufacture, distribution or possession of contraband products including tobacco and spirits; the illicit traffic of critical high technology and strategic good; and the enforcement of acts or regulations that impose non-tariff (permit) controls on the international movement of commodities.

♦ Drug Enforcement

This program manages the investigation of offenses related to the importation, exportation, manufacturing, cultivation, trafficking and possession of substances regulated by the Controlled Drugs and Substances Act in Canada. It provides International assistance and also administers and operates the RCMP's Drug Awareness program.

♦ Economic Crime

This program is committed to the delivery of police services in four main areas: commercial fraud, federal statutes and government programs, technological crime, and securities fraud. The focus is on those cases that involve substantial value or financial losses; that have a high degree of criminal sophistication; that requires special investigative expertise; or where the Government of Canada is a victim. Typical cases include business-related or white-collar crimes such as the corruption of public officials, breach of trust, land and mortgage fraud, bankruptcy and insolvency offences, employment insurance fraud, market manipulations, telemarketing fraud, currency and payment card counterfeiting.

♦ Federal Enforcement

This Federal Enforcement program is responsible for the investigation of a wide variety of federal statutes under five sub-programs. These are: Consumer Protection, including Copyright Enforcement, Weights and Measures and the Radiocommunication Act; Public Safety, including War Crimes and the Quarantine Act; Airport FES, including Airport and Marine Federal Enforcement; Environmental, including National Parks and Environmental Protection and Frauds against the Government, including Student Loans and the Canada Pension Plan.

♦ Immigration and Passport

Immigration and Passport Branch's strategy is to combat and disrupt illegal migrant smuggling and the trafficking in persons to Canada. This Program patnerships with federal government departments to provide an integrated approach to the enforcement of the Immigration and Refugee Protection Act, the Citizenship Act and the investigation of Canadian Passport violations under the Criminal Code.

♦ Proceeds of Crime

Proceeds of Crime (POC) objective is to disrupt criminal organization on a national and international level by identifying, restraining and forfeiting illicit and unreported wealth accumulated through criminal activity by investigating and prosecuting offenders.

♦ International Liaison and Protective Operations Directorate

This directorate is currently made up of the following branches: Liaison Officer Program, International Training and Peacekeeping, Prime Minister's Protection Detail, Protective Services, Strategic Activities and Interpol Program whose responsibilities are as follows:

- Liaison Officer Program: The Liaison Officer Program has RCMP members in strategic international locations to provide the Canadian and foreign law enforcement communities with assistance, information and coordinating support, especially for investigation on drugs, organized crime, proceeds of crime, commercial crime and immigration matters.
- International Training and Peacekeeping: This Program assists foreign countries in delivering effective and efficient law enforcement in keeping with Canada's interests to maintain the rule of law and combat crime. In support of Canadian foreign policy objectives, the RCMP CIVPOL Peacekeeping Operations is responsible for the selection, training, deployment and support of all Canadian police personnel participating in international police operations.
- Prime Minister's Protection Detail provides personal security to the Prime Minister and his family, protects the official residences, and when the Prime Minister travels abroad, ensures that the security measures provided by the host country meet Canadian standards.
- Protective Services directs the planning, implementation, administration and monitoring of the RCMP National Protective Security Program for the Governor General, her family and residences, the Prime Minister, his family and residences, federal Cabinet Ministers and their residences, Supreme and Federal Court Judges and their residences, Members of Parliament, Senators, visiting Heads of State, foreign diplomats in Canada and their residences, Internationally Protected Persons and persons designated by the Solicitor General of Canada as requiring security. It plans the security measures to be implemented during major events held in Canada. In addition, it monitors, analyses and provides timely advice to support the protective policing component at Vancouver, Edmonton and Halifax airports and directs the planning, implementation, training and monitoring of the Canadian Air Carriers Protective Program (CACPP).
- Strategic Activities provides strategic advice and planning, budgetary and personnel administration, support, communications, and management services for various Directorate programs and activities.
- Interpol Program: Canada's membership in the Interpol network and Interpol's National Central Bureau in Ottawa is the first contact point for inquiries from international law enforcement agencies and all Canadian police departments in the fight against organized crime and all criminal investigations requiring assistance from police agencies abroad and within Canada. The RCMP Interpol branch is comprised of police officers and civilian employees from the RCMP and various Canadian police agencies. Interpol in Ottawa provides assistance to Canadian and foreign police on matters including fraud, forgery, theft, drugs, smuggling, illegal immigration, missing persons, assault, auto theft, fugitive apprehension, dissemination of child pornography and stolen works of art.

RCMP Secretariat Activity

The Activity of Corporate Management includes the functions of strategic and corporate planning, corporate policy design, financial planning, audit and program evaluation. Responsiveness and accountability to the government are ensured by the coordination of communications, public affairs, information access, ministerial liaison and external review and appeals.

♦ Audit and Evaluation

This program is designed to plan, develop and implement a comprehensive audit approach to examine and review all RCMP law enforcement and administrative activities.

♦ Corporate Management

This program develops and coordinates strategic and corporate planning, formulates corporate policy, manages corporate information and conducts program evaluations and management studies. Annual accountability reports and briefings are developed for the Commissioner and in response to the government's planning process. The program is delivered through three components, Corporate Planning and Information Management, Strategic Planning and Corporate Policy, and Program Evaluation.

♦ External Review & Appeals

This program assists the Commissioner by providing advice, research and background material for all reviews and recommendations generated by the External Review Committee (ERC) and the Public Complaints Commission (PCC). The Sub-Activity also advises the Commissioner on appeals or grievances which must be considered by him, but which are not reviewed by an external agency.

♦ Finance and Supply

This program manages the financial affairs of the department to satisfy requirements for financial control and accountability of the RCMP, contracting partners, legislation and government. This program also provides internal support in accommodation, transport, food,

materiel and miscellaneous services for the RCMP in accordance with relevant policies, regulations and statutes.

♦ Public Affairs & Information

This program aims at promoting good public relations, conveying and protecting an accurate and constructive image of the RCMP in Canada and abroad. Initiatives include the provision of information and responses to requests from the general public regarding RCMP activities, the handling of visits of policing personnel from around the world, participation in public events at the national and international levels as part of our Canadian Heritage, the maintaining of contemporary and historical materials, the management of the Musical Ride program, the management of partnerships and sponsorships from the private and the public sectors, the management of RCMP Licensing Products and RCMP Intellectual Property. Furthermore, this program also manages a centralized response area to requests made under the Access to Information and Privacy Acts for access to records under the control of the RCMP. The sub-Activity develops policies and procedures to ensure conformity with the legislation while maintaining the protection of sensitive information and the privacy of individuals.

Information Holdings

Program Records

Linking Statement

All records retained by the RCMP are subject to one classification methodology. Records are retained in accordance with the subject content of the record, based on a central file classification system, rather than function or activity. Each Detachment, Sub-Division, Division and Headquarters, Ottawa classifies records under three main groups, Administrative, Operational Policy, and Sequential (Operational Investigative Records). The Administrative records are divided into seven sub-classifications. These are further categorized, as are the Operational Policy records, into sub-topics, which are standard throughout the RCMP. The Sequential (Operational Investigative Records) pertain to the general investigative records generated and retained at each site, and as the name suggests, each is sequentially numbered. The volume of records will vary from location to location, however the retention system is uniform. This system is centrally regulated and this enables the RCMP to describe its record holdings in the three distinct categories. Requesters need only describe the record they wish to access. If the request pertains to a specific incident, the location of that incident is also required.

Administration - Buildings & Real Property Records
Description: Headquarters, Directorates, Divisions, Sub-Divisions and Detachments each may have administrative records of a policy and/or routine nature pertaining to the acquisition, disposition and rental of lands and buildings and the services supplied to lands and buildings owned or leased by the RCMP. ***Topics:*** Buildings & Real Property - General; Buildings & Works - General; Buildings & Works - Estimates; Building and Works by Division; Buildings - Telecommunication Shelters; Buildings - Janitorial Contracts; Buildings & Properties Management Service Agreements; Real Property - General; Real Property - Police Owned (other than Telecom. Sites); Real Property - Police Rented or Leased (other than Telecom. Sites); Real Property - Cemeteries & Graveyards; Real Property - Telecom. Sites Owned; Real Property - Telecom. Sites Leased or Rented; Real Property - Historical Sites & Monuments; Utilities - other than Telephone Services. ***Program Record Number:*** CMP ADM 006

Administration - Equipment & Supplies Records
Description: Headquarters, Directorates, Divisions, Sub-Divisions and Detachments each may have administrative records of a policy and/or routine nature pertaining to the supply, maintenance and repairs of RCMP equipment and supplies. ***Topics:*** Equipment & Supplies (General); Accounting & Inventories; Aircraft; Aircraft Supplies & Equipment; Buildings & Living Accommodation, including Furniture & Furnishings; Cataloguing, Identification & Labelling of equipment and supplies; Clothing & Kit (condemning, destruction, repayment issues, alterations); Clothing & Kit - Purchase Descriptions; Clothing & Kit - Design Specifications, Authorities & Approvals; Clothing & Kit - Issues & Receipts; Clothing & Kit - Material and Clothing; Clothing & Kit - Testing & Samples; Condemnation & Destruction; Firearms & Weapons (issues and repairs); Ammunition; Enquiries & Information (concerning uniforms, equipment and supplies); Loans (of uniforms and equipment); Material Specifications; Procurement & Purchases; General Stores; Micrographic Equipment & Supplies; Office Machines; Office Furniture & Furnishings; Printing & Duplicating Equipment; Stationery & Office Supplies; Technical Equipment Evaluations; Telecommunication Equipment Evaluations; Computer Equipment, Hardware and Software; Riot & Crowd Control Equipment; Water Transport & Outboard Motors; and Vehicles (purchase, maintenance, repair licensing, insurance, credit card system and disposal). ***Program Record Number:*** CMP ADM 005

Administration - Financial Records
Description: Headquarters, Directorates, Divisions, Sub-Divisions and Detachments each may have administrative records of a policy and/or routine nature

pertaining to the financial matters of the RCMP. ***Topics:*** Finances (General); Accounting; Accounting - Cash; Accounts Payable - Commercial Firms & Supplies - Other Government Departments, or Police Departments - Utilities; Accounts Receivable - General - Policing; Acts, Directives and Orders; Allowances & Deductions; Banks & Banking; Budgets & Budgeting; Cheques; Coding (Financial Coding Systems); Contingency Account; Estimates; Fees (consultant, professional, tuition, membership, etc.); Funds (Benefit Trust Fund); Grants; Postage; Signing Authorities; Taxes; Transfer Expenses; Transport Requisitions; Travelling Expenses. ***Program Record Number:*** CMP ADM 004

Administration - General Administration Records
Description: Headquarters, Directorates, Divisions, Sub-Divisions and Detachments each may have administrative records of a policy and/or routine nature pertaining to the organization, administrative history and policy of the RCMP. ***Topics:*** General Administration; Abbreviations, Designations and Titles; Accidents; Addresses and Speeches; Briefings and Presentations; RCMP Acts and Regulations; Agreements for Policing Services; Aboriginal Policing; Appreciation, Condolences, Greetings; Associations and Societies; Corporate Identity Program; Badges, Flags and Colours; Cafeterias; Canteens; Messes; Campaigns and Canvassing; Cemeteries, Graves and Memorials; Ceremonies and Celebrations; Claims (on behalf or against the Crown); Complaints against the RCMP; Conferences and Committees; Cultures and Customs; Dress Regulations; Emergency Planning; Gifts and Presentations to/from RCMP; Audits; Inspections and Evaluations; Reviews and Overviews; Inventions and Patents; Copyright; Licences, Passes and Permits; Museums, Relics and Curios; Official Languages; RCMP Organization; Headquarters Organization; Division Organization; RCMP Planning Process; Manuals; Commissioner's Bulletin; Pony Express; Reports and Returns; Commissions; Saluting and Compliments; Sports and Recreation Clubs (RCMP). ***Program Record Number:*** CMP ADM 001

Administration - General Services Records
Description: Headquarters, Directorates, Divisions, Sub-Divisions and Detachments each may have administrative records of a policy and/or routine nature pertaining to services that support the administration and operation of the RCMP. ***Topics:*** General Services; Office Services; Artisan Services; Correspondence Management; Directives Management; Data Processing Services (general); Standards and Documentation; Software and Operations; Data Transmission; Operations; Automated Systems; Projects & Studies; Systems Research & Planning; Systems Integration; CPIC Services; Forms Management; Graphic Arts Management; Horses; Liaison and Public Relations - General; Liaison - Solicitor and Attorneys General; Liaison with Other Government Departments and Outside Agencies; Liaison with Other Police Forces; Liaison Internal; Liaison - Police Community Relations; Exhibitions (by and participated in by RCMP, eg. CNE, Calgary Stampede, etc.); Historical (history of and articles about RCMP); Visits and Tours to/by RCMP; RCMP Quarterly; Library Services; Mail Management; Management Services; Micrographic Services; Program Evaluation; Performance Measurement; Photographic Services; Printing and Duplication; Publications; Records Management; Records Filing Systems; Records Disposition; Research and Development Management; RCMP Band; RCMP Gazette; RCMP Musical Ride; Security (non-operational, internal security only); Organizational and Administrative Security (threat and risk assessment); Personnel Security (security screening and clearances); Physical Security (RCMP buildings etc.); Communications Security; EDP Security; Telecommunications; Telecommunication Projects; Radio Services; CCTV Services; Transmission Services; Telephone Services; Interoffice Communications; Translation Services; Transportation and Accommodation; Police Service Dogs; Forensic Services - General - Alcohol - Chemistry - Counterfeit Detection - Document Examination - Firearms and Ammunition Examination - Forensic Drugs - Hair and Fibre - Serology - Toxicology - Radiography - Social Science - Photography - Identification (eg. facial reconstruction, fingerprints, footwear, dentures, genetic fingerprinting) - Analytical Services (lab automated systems). ***Program Record Number:*** CMP ADM 007

Administration - Personnel Records - Public Service and Municipal Employees
Description: Headquarters, Directorates, Divisions, Sub-Divisions and Detachments each may have administrative records of a policy and/or routine nature pertaining to Public Service and municipal Employees of the RCMP. ***Topics:*** Public Service and Municipal Employees records, general; Acts & Regulations; Accidents & Injuries; Hours of Work; Bulletins & Circulars; Classification; Classification, Position files; Collective Bargaining; Conduct, Discipline & Grievances; Competitions; Employment General; Evaluation & Performance Rev.; Health & Medical; Income Tax; Insurance; Leave & Holidays; Pay, Salaries & Wages; Pension; Transfers. ***Program Record Number:*** CMP ADM 003

Administration - Personnel Records - RCMP Members
Description: Headquarters, Directorates, Divisions, Sub-Divisions and Detachments each may have administrative records of a policy and/or routine nature pertaining to the records dealing with members of the RCMP. ***Topics:*** RCMP Personnel (Members Records); Accidents & Injuries (other than RCMP Transport); Appointments; Awards & Honours (including PS & municipal employees); Suggestion Awards;

Classification (RCMP General); Classification Standards; Delegation of Classification and Monitoring; Classification of Position Files; Complaints against and by members of the RCMP; Debts & Loans; Discharge of firearms in the Course of Duty; Discharge & Retirements; Discipline and Conduct - Adjudication Boards and Damage to or Loss of Government Property (boards or investigations); Establishment (including PS Employees); Evaluation & Performance Reviews; Staffing; Health & Medical Services; Member Assistance Program; Occupational & Environmental Health & Safety (regulations); Hours of Work; Inquiries & Information on personnel (including PS & Municipal Employees, serving and ex-members, etc); Income Tax; Insurance; Leave; Morale; Oaths of Allegiance and Secrecy (including PS & Municipal Employees); Passports and Visas, arrangements for (including PS & Municipal Employees); Pay, Bonus & Salaries; Pensions; Personnel Management Info. System (PARADE); Privileges; Promotions; Recruiting and Employment; Temporary Civilian Employees (guards, matrons, etc.); Succession Planning; Training and Development, General (including PS & Municipal Employees) - Foreign Govt. Assistance, Centralized, Canadian Police College Research & Program Development, Divisional, Offered outside the RCMP (Language and university); Training - Recruit; Transfers (northern service). ***Program Record Number:*** CMP ADM 002

Operational Investigative Records
Description: Headquarters and Directorates in Ottawa, Divisions, Sub-Divisions and Detachments each may have sequential, investigational records relating to protective services, occurrences reported to, and/or under investigation by the RCMP. ***Topics:*** Occurrences & Investigations including statements, exhibit reports, copies of court documents and in some instances records relating to criminal histories & intelligence and related documentation pertaining to offenses under the: Criminal Code, Federal Statutes, Provincial Statutes, Municipal By-Laws and Territorial Ordinances; Occurrences & Investigations providing assistance to Multi jurisdictional Authorities, Foreign Authorities, Federal Authorities, Provincial Authorities, Municipal Authorities, Territorial Authorities, Private Companies and the General Public; V.I.P. Protection (Foreign and Canadian); Threats made against the country and the police. ***Program Record Number:*** CMP INV 001

Operational Policy Records
Description: Headquarters and Directorates in Ottawa, Divisions, Sub-Divisions and Detachments each may have records concerning the instructions and interpretations of policy relating to the enforcement of statutes and regulations, and the policy relating to cooperation with governments, foreign law enforcement authorities and the general public. ***Topics:*** General policy subjects; Counsel (appointment, transportation and co-operation with); Fines & Costs (collection and disposition); Prisoners & Mental Patients (custody, transportation, searching); Exhibits (custody and disposition); Correspondence (crime reports); Human Sources; Jurisdiction; Laws (enforcement and amendments); Cooperation with and Assistance to Foreign Authorities, Federal authorities, Provincial authorities, Territorial Authorities, Municipal Authorities, Private Companies, and the General Public; Criminal Intelligence Branch; Securities Fraud Information Centre; Special Services Branch; V.I.P. Protection; Threat Assessments - police - Country. ***Program Record Number:*** CMP OPS 001

Standard Program Records

Please see the INTRODUCTION to this publication for the definition of Standard Program Records and a description of their contents.

Accounts and Accounting
Administration
Budgets
Buildings and Properties
Classification of Positions
Employment and Staffing
Equipment and Supplies
Finance
Furniture and Furnishings
Human Resources
Lands
Occupational Health, Safety and Welfare
Office Appliances
Official Languages
Pensions and Insurance
Personnel
Procurement
Salaries and Wages
Staff Relations
Training and Development
Utilities
Vehicles

Personal Information Banks

♦ Personnel (RCMP)

Applicants' Records
Description: The file and the Human Resource Management Information System (HRMIS) contains such material as applicant evaluations, selection test score, candidate assessments, engagement check sheet, pare certification and related correspondence, personnel interview report data update. Information on successful applicants who are enrolled by the RCMP is placed on a Cadet file. Information on successful applicants who are engaged in the RCMP is placed in

the member performance review and appraisal records (CMP PPE 801), service records (CMP PPE 802) and medical records (CMP PPE 808). In addition to the requirements indicated on the Personal Information Request Form, individuals must provide their full name, date of birth and the location where the last application was made. Individuals wishing to access only specific information should identify the material desired to expedite the processing of their requests. Security/Reliability screening records have to be accessed via CMP PPU 065. Complaints dealing with the suitability of individuals may be found in bank CMP PPU 085. ***Class of Individuals:*** This bank contains personal information on individuals who have applied for engagement in the RCMP as regular members, special constable members or civilian members. ***Purpose:*** This information is used to determine the suitability of individuals for engagement in the RCMP. ***Consistent Uses:*** This information is also used for research, planning, evaluation statistics and may also be matched with the following information banks: CMP PPE 090 (Honours and Awards), CMP PPE 804 (Member Grievance Records); CMP PPE 803 (RCMP Member Promotion Board Proceedings Records); CMP PPE 805 (RCMP Member Discipline Records); CMP PPU 085(Complaints Against the RCMP or a Member, Enquiries and General Assistance); CMP PPE 806 (RCMP Member's Pay and Allowance Records); CMP PPE 815 (RCMP Member Conflict of Interest and Post Employment Code Records); CMP PPE 818 (Employment Equity Program). All linkages for the purpose of administering human resources and compensation plans are in compliance with the provisions of the Privacy Act. ***Retention and Disposal Standards:*** Information on unsuccessful applicants is maintained for a period of five calendar years at the headquarters of the division to which they applied. ***RDA Number:*** 2000/030 ***Related to PR#:*** CMP CMP 920 ***TBS Registration:*** 001008 ***Bank Number:*** CMP PPU 070

Complaints Against the RCMP or a Member, Enquiries and General Assistance

Description: This bank contains Part VII RCMP Act investigations and criminal investigation reports, occurrence reports, voluntary statements of members, statements of witnesses and complainants, and related correspondence of members and complainants. In addition to the requirements indicated on the Personal Information Request Forms, individuals must provide their full name, date of birth, sufficient detail of the occurrence, and the geographic location where the information search is to be conducted. Individuals wishing to access only specific information should identify the material desired, to expedite the processing of their requests. Part VII RCMP Act investigations dealing with complaints from the public and which result in discipline against a member may be located in bank CMP PPE 805. ***Class of Individuals:*** This bank contains personal information on individuals who have been involved in complaints against the RCMP or its members, general enquires by the public concerning the RCMP, and cases of general assistance to the public by the RCMP. ***Purpose:*** This information is used for the internal administration of the RCMP. ***Consistent Uses:*** The RCMP External Review Committee and the RCMP Public Complaints Commission may use the information respectively to enquire into grievances and investigate complaints against the RCMP or its members. Information in this bank is also used for research, planning, evaluation, press releases and statistical purposes. ***Retention and Disposal Standards:*** Information in this bank is retained for a minimum of two calendar years. Where the record has been designed as having archival or historical value, the record shall be transferred to the control of the National Archives of Canada; and where the record has not been so designated, it shall be destroyed. ***RDA Number:*** 89/025, 96/023, 96/024 ***Related to PR#:*** CMP CMP 918 ***TBS Registration:*** 001011 ***Bank Number:*** CMP PPU 085

Honors and Awards

Description: This bank contains recommendations, supporting material, social insurance numbers (SIN) in some cases, and any assessments relating to the granting of an honour or award. The SIN is collected under the authority of the FAAS-7 for the purpose of maintaining information relative to the Treasury Board (TB) Recognition Policy. In addition to the requirements indicated on the Personal Information Request Form, individuals must provide the geographic location and sufficient detail of circumstances as may relate to them. Individuals wishing to access only specific information should identify the material desired, to expedite the processing of their requests. ***Class of Individuals:*** This bank contains personal information on individuals who have been recommended for an honour or award (usually for an act of bravery or distinguished service to the country), where the RCMP has provided supporting data to the issuing authority. ***Purpose:*** This information is used by the issuing authorities of various honours and awards programs to assist in determining whether or not to grant an honour or award. The SIN is used/collected for the purpose of issuing awards (cheque and T4 - 1A slip for income tax purposes) under the TB Recognition Policy, Canadian Honours System and RCMP Long Service Medal Regulations. ***Consistent Uses:*** This information may also be used for research, planning, evaluation and statistics and may also be matched with the following information banks: CMP PPE 070 (Applicants' Records); CMP PPE 801 (RCMP Member Performance Review and Appraisal Records); CMP PPE 802 (RCMP Member Service Records); CMP PPE 803 (RCMP Member Promotion Board Proceedings Records); CMP PPE 805 (RCMP Member Discipline); CMP PPU 085 Complaints Against the RCMP or a Member, Enquiries and General

Assistance); CMP PPE 806 (RCMP Member's Pay and Allowance Records); CMP PPE 815 (RCMP Member Conflict of Interest and Post Employment Code) and CMP PPE 818 (Employment Equity Program); CMP PPE 804 (RCMP Member Grievance Records). All linkages for the purpose of administering human resources and compensation plans are in compliance with the provisions of the Privacy Act. ***Retention and Disposal Standards:*** Information in this bank is retained for a minimum of three calendar years. Where the record has been designated as having archival or historical value, the record shall be transferred to the control of the National Archives of Canada; and where the record has not been so designated, it shall be destroyed. ***RDA Number:*** 89/013, 96/024 ***Related to PR#:*** CMP CMP 918 ***TBS Registration:*** 001012 ***Bank Number:*** CMP PPU 090

RCMP Police Car Accidents/Claims By or Against the RCMP

Description: This bank contains investigational and occurrence reports, statements, claims for damages, legal decisions and related documentation. In addition to the requirements indicated on the Personal Information Request Form, individuals must provide sufficient detail of their contact with the RCMP including the date, nature and geographic location of the occurrence. Individuals wishing to access only specific information should identify the material desired, to expedite the processing of their requests. ***Class of Individuals:*** This bank contains personal information on individuals who have been involved in RCMP transport accidents, assessment and/or demands respecting damage or loss in relation to property, and other similar claims by or against the RCMP. ***Purpose:*** This information is used to determine liability for motor vehicle accidents and to process damage settlements. ***Consistent Uses:*** Information in this bank is also used for the internal administration of the RCMP, research, planning, evaluation and statistics and may also be matched with the following information banks: CMP PPE 070 (Applicants' Records); CMP PPE 801 (RCMP Member Performance Review and Appraisal Records); CMP PPE 802 (RCMP Member Service Records); CMP PPE 803 (RCMP Member Promotion Board Proceedings Records); CMP PPE 805 (RCMP Member Discipline); CMP PPU 085 (Complaints Against a the RCMP or a Member, Enquiries and General Assistance); CMP PPE 806 (RCMP Member's Pay and Allowance records); CMP PPE 815 (RCMP Member Conflict of Interest and Post Employment Code), CMP PPE 818 (Employment Equity Program) and CMP PPE 804 (RCMP Member Grievance Records). This information may be matched with information from other personal information banks and/or program records. All linkages for the purpose of administration or enforcement of the law and in the detection, prevention or suppression of crime are in compliance with the provisions of the Privacy Act. ***Retention and Disposal Standards:*** Information in this bank is retained for a minimum of two calendar years. Where the record has been designated as having archival or historical value, the record shall be transferred to the control of the National Archives of Canada; and where the record has not been so designated, it shall be destroyed. ***RDA Number:*** 89/013, 95/009, 96/023, 96/024 ***Related to PR#:*** CMP SSD 913 ***TBS Registration:*** 001009 ***Bank Number:*** CMP PPU 075

♦ Information and Identification Services

Criminal Records, Summaries of Police Information, and Identification Fingerprints

Description: This bank contains criminal records (convictions and discharges certifiable under Section 667 of the Criminal Code of Canada), summaries of police information related to other charges and their dispositions, Pardoned Records, fingerprints, and related correspondence identifiable by fingerprints. It also contains identification fingerprints pursuant to the Immigration Regulations, 1978 and fingerprints of employees of the RCMP and the CSIS. In addition to the requirements indicated on the Personal Information Request form, individuals who wish copies of their (a) criminal record, (b) summary of police information related to them or (c) Pardoned record, must forward identifiable fingerprints to: the Director, Information & Identification Services, RCMP, Box 8885, Ottawa, Ontario, K1G 3M8, specifying their requirement for a criminal record only, both criminal record and summary of police information and/or their Pardoned Record. The request will be treated informally and will be responded to as soon as practicable. These fingerprints are used for the purposes of search and positive identification only, and will be returned with the access request results. Information in this bank may be maintained in hard copy files, microfilm electronic images as well as in automated form in the Canadian Police Information Center (CPIC) and/or in the Criminal Record Entry Maintenance and Monitoring - Direct Entry System (CREMM - DES). Records are held at RCMP Headquarters and various external RCMP detachments. ***Class of Individuals:*** Individuals who have been fingerprinted as a result of criminal charges, individuals fingerprinted under the Immigration Regulations, 1978 and employees of the RCMP and the CSIS. ***Purpose:*** Law enforcement, security/reliability clearances and identification purposes. ***Consistent Uses:*** This information is used by domestic and foreign law enforcement and investigative agencies of federal/provincial/state and municipal governments, departments of the criminal justice system and the courts, in the administration or enforcement of the law and in the detection, prevention or suppression of crime generally. This information is used by the insurance crime prevention bureaus for the purpose of combating arson and auto theft and related offences, by the federal/provincial/municipal agencies for security and reliability screening, by the Canadian Security

Intelligence Service for the purposes of investigating threats to the security of Canada and the preparation of security assessments. This information is also used for research planning, evaluation and statistical purposes and may be matched with information from other personal information banks and/or program records. All linkages for the purpose of administration or enforcement of the law and in the detection, prevention or suppression of crime are in compliance with the provisions of the Privacy Act. Fingerprints taken under authority of the Immigration Regulations, 1978 are used for identification purposes in the immigration process. RCMP and CSIS employee fingerprints are used to assist in the maintenance of continuously updated security/reliability clearances. ***Note:*** Pardoned Records will be released only to individuals entitled to these records under the Privacy Act or with the approval of the Solicitor General of Canada. ***Retention and Disposal Standards:*** The personal information contained in this bank is broken down into several categories. The National Archivist of Canada has assigned each of these categories a corresponding retention schedule which can vary from several months to the time data subject reaches the age of one hundred years. Where the record has been designated as having archival or historical value, the record shall be transferred to the control of the National Archives of Canada; and where the record has not been so designated, it shall be destroyed. ***RDA Number:*** 91/015, 96/023 ***Related to PR#:*** CMP IDD 105 ***TBS Registration:*** 001002 ***Bank Number:*** CMP PPU 030

Restricted Weapon Registration System (RWRS)
Description: This data bank contains applications to register restricted weapons, registration certificates, and other weapons that are recorded to police agencies, government departments, museums, firearms dealers and others, interprovincial permits to carry, transport or convey restricted weapons as was required under former Part III of the Criminal Code of Canada (prior to 98-12-01). The data bank also contains documentation on prohibition orders, refusals and revocation of registration certificates and interprovincial permits to carry. Under the Firearms Act, the records kept in the registry by the Commissioner of the RCMP under former Part III of the Criminal Code of Canada are transferred to the Registrar who has the authority to maintain a registry of every Firearms Registration Certificate. In addition to the requirements on the Personal Information Request Form, individuals must provide their full name, date of birth and address. Information in relation to registration certificates, refusals or revocations of registration certificates, and interprovincial permits to carry restricted weapon(s) is located at RCMP headquarters in Ottawa. Information relating to FAC's, other permits, certificates and prohibitions is located at the detachment or unit level. Individuals wishing to access information not held in Ottawa must indicate the location and/or the name of the RCMP unit where the application was made, or the permit or certificate issued. Individuals wishing to access only specific information should identify the material desired, to expedite the processing of their requests. Information in this bank may be maintained in hard copy, on microfilm, and in automated form in the Canadian Police Information Center (CPIC). ***Class of Individuals:*** Individuals who have applied to register restricted weapons in Canada and have been issued a registration certificate; applied to the local registrar (L.R.) of firearms for a permit to carry/convey/transport a restricted weapon in Canada; been refused or have had a permit or certificate revoked; or have been prohibited from possessing firearms. ***Purpose:*** The administration and enforcement of firearms control legislation in Canada. ***Consistent Uses:*** Information in this bank is used by domestic and foreign accredited law enforcement of federal, provincial/state and municipal governments, and chief provincial/territorial firearms officers, in the administration or enforcement of the law and in the detection, prevention or suppression of crime in general. This information may be matched with information from other personal information banks and/or program records. All linkages for the purpose of administration or enforcement of the law and in the detection, prevention or suppression of crime are in compliance with the provisions of the Privacy Act. ***Retention and Disposal Standards:*** Information in this bank is retained for a minimum of ten calendar years. Some personal information in this bank may be retained permanently pursuant to the Firearms Records Regulations. Where the record has been designated as having archival or historical value, the record shall be transferred to the control of the National Archives of Canada; and where the record has not been so designated, it shall be destroyed. ***RDA Number:*** 69/123, 95/009, 96/023 ***Related to PR#:*** CMP IDD 110 ***TBS Registration:*** 005045 ***Bank Number:*** CMP PPU 035

Canadian Firearms Registration System (CFRS)
Description: This data bank contains applications to register non-restricted, restricted and prohibited firearms, registration certificates and other firearms that are recorded to police agencies, government departments, and others, interprovincial and international carrier licences, the names of the individuals who are approved verifiers and authorizations to import and export by firearm dealers as required under the Firearms Act (beginning 98-12-01). The data bank also contains documentation on refusals and revocation of registration certificates, interprovincial and international carrier licences and authorizations to import and export. The Registrar has the statutory authority under the Firearms Act to maintain a registry of every Firearm Registration Certificate. In addition to the requirements on the Personal Information Request Form, individuals must provide their full name, date of birth and address.

Information in relation to registration certificates, refusals or revocations of registration certificates, and interprovincial and international carrier licences and authorizations to import and export is located at RCMP headquarters in Ottawa. Information relating to firearms licences, other authorizations and prohibitions is located at the Chief Firearms Officer (CFO) or detachment level where applicable. Individuals wishing to access information not held in Ottawa must indicate the location and/or the name of the CFO or RCMP unit where the application was made, or the licence or authorization issued. Individuals wishing to access only specific information should identify the material desired, to expedite the processing of their requests. Information in this bank may be maintained in hard copy, on microfilm, in automated form in the Canadian Police Information Center (CPIC), File Management System (FMS), or in the Canadian Firearm Registration System (CFRS). - The CFRS data bank also contains applications from individuals or business' regarding licences and authorizations that are issued or revoked and applications for licences or authorizations that are refused by the CFO. The data bank also contains documentation on prohibition orders of which the CFO is informed under Section 89 of the Firearms Act. The CFO has the statutory authority under the Firearms Act to maintain a registry of every licence or authorization applied for under the said act. In addition to the requirements on the Personal Information Request Form, individuals must provide their full name, date of birth and address. Information in relation to licences and authorizations that are issued or revoked, applications for licences or authorizations that are refused and documentation on prohibition orders of which the CFO is informed under Section 89 of the Firearms Act are located at each provincial headquarters of the CFO's. Individuals wishing to access information not held in Ottawa must indicate the location and/or the name of the Federal CFO where the application was made, or the licence or authorization issued. Individuals wishing to access only specific information should identify the material desired, to expedite the processing of their requests. Information in this bank may be maintained in hard copy, on microfilm and in the automated form in the Canadian Police Information Center (CPIC) or in CFRS. ***Class of Individuals:*** Individuals who have applied to register non-restricted, restricted or prohibited firearms in Canada and have been issued a registration certificate or been refused or have had a licence, authorization or certificate revoked. - Individuals or business' who have applied or been refused or have had a licence, authorization or certificate revoked; or have been prohibited from possessing firearms. ***Purpose:*** The administration and enforcement of firearms control legislation in Canada. ***Consistent Uses:*** Information in this data bank is used by domestic and foreign accredited law enforcement of federal, provincial/state and municipal governments and Chief Firearms Officers, in the administration or enforcement of the law and in the detection, prevention or suppression of crime in general. This information may be matched with information from other personal information banks and/or program records. All linkages for the purpose of administration or enforcement of the law and in the detection, prevention or suppression of crime are in compliance with the provisions of the Privacy Act. ***Retention and Disposal Standards:*** Information in this bank is retained for a minimum of ten calendar years. Some personal information in this bank may be retained permanently pursuant to the Firearms Records Regulations. Where the record has been designated as having archival or historical value, the record shall be transferred to the control of the National Archives of Canada; and where the record has not been designated, it shall be destroyed. ***TBS Registration:*** 005046 ***Bank Number:*** CMP PPU 037

Operations Activity

Courses Administered by the RCMP

Description: This bank contains a record of nominal rolls, in some cases assessments including examinations, tests and other forms of performance measures and related documents. This bank also contains personal information on public servants employed by the RCMP, including their social insurance number (SIN), who have participated in courses administered by the RCMP or sponsored by an outside agency. It also includes the SIN of RCMP members who have participated in Public Service Commission (PSC) courses. The information is collected under the authority of the Public Service Staff Relations Act and the Public Service Employment Act. For members of the RCMP, assessments are also maintained on their personnel file (Bank CMP PPE 801). In addition to the requirements indicated on the Personal Information Request Form, individuals must provide their full name, regimental number if applicable, the title, location and date of the course as well as whether they were an instructor or candidate. Individuals wishing to access only specific information should identify the material desired, to expedite the processing of their requests. ***Class of Individuals:*** This bank contains personal information on individuals who have applied for or attended, as candidates or instructors, training and development or educational courses administered by the RCMP, the PSC, the National Archives Canada, or other Training/Educational Institutions that are centrally controlled through registration procedures by the RCMP. ***Purpose:*** This information is used to support qualifications for certificates, awards or diplomas, determine the eligibility of candidates for future courses and support the renewal of an instructor's personal service contract. The information pertaining to public servants' and RCMP members' social insurance numbers is for the purpose of managing training throughout the public service and for administering courses provided by the PSC Training and Development Canada.

Consistent Uses: This information is also used for research, planning, evaluation and statistics and may be matched with the following information banks: RCMP Member Performance Review annd Appraisal Records (CMP PPE 801), RCMP Member Promotion Board Proceedings Records (CMP PPE 803), RCMP Grievance Records (CMP PPE 804), RCMP Member Discipline Records (CMP PPE 805); CMP PPU 085 (Complaints Against the RCMP or a Member, Enquiries and General Assistance); Employment Personnel Records (CMP PSE 901), Staffing (CMP PSE 902), Training and Development (CMP PSE 905), Grievances (CMP PSE 910), Discipline (CMP PSE 911), Performance Reviews and Employee Appraisals (CMP PSE 912). All linkages for the purpose of administration or enforcement of the law and in the detection, prevention or suppression of crime are in compliance with the provisions of the Privacy Act. ***Retention and Disposal Standards:*** Information in this bank is retained for a minimum of five calendar years. Where the record has been designated as having archival or historical value, the record shall be transferred to the control of the National Archives of Canada; and where the record has not been so designated, it shall be destroyed. ***RDA Number:*** 95/009, 95/011, 96/023, 96/024, 98/005 ***Related to PR#:*** CMP CMP 927 ***TBS Registration:*** 001010 ***Bank Number:*** CMP PPU 080

♦ Community, Contract and Aboriginal Policing

Community Policing Services

Description: This bank contains personal information on individuals involved in regional RCMP crime prevention/police community relations programs such as the RCMP Summer Student Program or other divisional crime prevention programs. Such programs are intended to prevent and control the incidence of crime and protect life and property and to provide the candidates with the opportunity to interface with the police function and criminal justice system as a whole. This bank contains applications, written terms of involvement, and any other record used in accepting or rejecting an individual to participate in such a program. Information in this bank is not generally carded or indexed to an individual. In addition to the requirements indicated on the Personal Information Request Form, individuals must provide sufficient detail of their involvement in the RCMP program, including the geographic location, dates and name of the program, to retrieve information of interest. Individuals wishing to access only specific information should identify the material desired, to expedite the processing of their requests. ***Class of Individuals:*** Individuals who have applied for and served in regional RCMP community relations/crime prevention programs. ***Purpose:*** This information is used to determine the suitability of individuals to participate in RCMP community relations/crime prevention programs. ***Consistent Uses:*** The information is also used for research, planning, evaluation and statistical purposes and may be matched with information from other personal information banks and/or program records. All linkages for the purpose of administration or enforcement of the law and in the detection, prevention or suppression of crime are in compliance with the provisions of the Privacy Act. ***Retention and Disposal Standards:*** Records within this bank are retained by the home division for a minimum of two years following termination of service or participating in program. ***RDA Number:*** 69/164, 96/023 ***TBS Registration:*** 000998 ***Bank Number:*** CMP PPU 010

♦ Criminal Intelligence

Criminal Operational Intelligence Records (Exempt bank)

Description: This bank contains personal information on individuals who have been implicated, following criminal investigations, in organized crime activities such as drug trafficking, securities fraud, corruption, counterfeiting, extortion, gambling, loan sharking, pornography and prostitution. Also included in this bank are records containing personal information concerning administration, policy and management of confidential human sources and witnesses requiring protection relating to criminal operations. This bank contains investigations and occurrence reports, statements and related documentation. This bank is designated by the Governor-in-Council as an exempt bank pursuant to Section 18(1) of the Privacy Act, on the basis of section 22 of the Act. Information in this bank may be maintained in hard copy files as well as in automated form such as Automated Criminal Intelligence Information System (ACIIS) and FOCUS, Police Information Retrieval System (PIRS), Police Reporting Occurrence System (PROS), National Criminal Data Bank (NCDB) and Division Information Bank (DIB). ***Class of Individuals:*** Individuals implicated in, or who are connected with and are the subject of criminal investigations including confidential human sources and witnesses. ***Purpose:*** Compiled in the administration or enforcement of the law and in the detection, prevention or suppression of crime generally. ***Consistent Uses:*** The information is used by accredited domestic and foreign law enforcement and investigative agencies in the administration or enforcement of the law and in the detection, prevention or suppression of crime generally. Personal information concerning human sources and witnesses is used in the administration and management of these individuals. This information is also used by federal departmental security officers for security and reliability screening, as well as for research, planning, evaluation and statistical purposes and may be matched with information from other personal information banks and/or program records. All linkages for the purpose of administration or enforcement of the law and in the detection, prevention or suppression of crime are in compliance with the provisions of the

Privacy Act. ***Retention and Disposal Standards:*** Records within this bank are retained for a minimum of two calendar years. Where the record has been designated as having archival or historical value, the record shall be transferred to the control of the National Archives of Canada; and where the record has not been so designated, it shall be destroyed. ***RDA Number:*** 95/009, 95/011, 93/024, 99/006 ***Related to PR#:*** CMP CIS 095 ***TBS Registration:*** 000999 ***Bank Number:*** CMP PPU 015

National Security Investigations Records (Exempt bank)
Description: This bank contains personal information about individuals who come to the attention of the RCMP in the course of national security enforcement including information collected in the fulfilment of the primary responsibility conferred by subsection 6(1) of the Security Offenses Act, more particularly information obtained or prepared for investigation purposes in respect of an offence under any law of Canada where a) the alleged offence arises out of conduct constituting a threat to the security of Canada within the meaning of the Canadian Security Intelligence Service Act, or b) the victim of the alleged offence is an internationally protected person within the meaning of section 2 of the Criminal Code, or the apprehension of the commission of such an offence. This bank also contains security assessments relating to internationally protected persons, as well as information concerning the management of protection services for confidential sources and witnesses used in national security investigations. This bank is designated by the Governor-in-Council as an exempt bank pursuant to Section 18(1) of the Privacy Act, on the basis of section 22 of the Act. Information in this bank may be maintained in hard copy files as well as in automated form on the Secure Criminal Information System (SCIS). ***Class of Individuals:*** Individuals who come to the attention of the RCMP during the course of national security enforcement, including fulfilment of the primary responsibility pursuant to subsection 6(1) of the Security Offenses Act, internationally protected persons, and persons providing confidential information in security investigations. ***Purpose:*** Information in this bank is used by the RCMP whose duties involve the enforcement of the law and the prevention of crime in carrying out its mandate and responsibilities in relation to national security enforcement and for the purposes of security and reliability screening. ***Consistent Uses:*** The information is used in the course of national security enforcement including fulfilment of the RCMP's primary responsibility conferred by subsection 6(1) of the Security Offenses Act. Information is required to carry out their mandate and responsibilities in relation to national security investigations and for security and reliability screening. Information in this bank is used by domestic and foreign law enforcement and investigation agencies in connection with their official duties and responsibilities in relation to the enforcement or administration of the law and to carry out their mandate and responsibilities in relation to national security investigations. It is also used by CSIS and other federal department security officers for security and reliability screening. It is also disclosed to domestic and foreign law enforcement and investigative agencies in connection with national security investigations. This information may be matched with information from other personal information banks and/or program records. All linkages for the purpose of administration or enforcement of the law and in the detection, prevention or suppression of crime are in compliance with the provisions of the Privacy Act. ***Retention and Disposal Standards:*** Records within this bank are retained for a minumum of five calendar years. Where the record has been designated as having archival or historical value, the record shall be transferred to the control of the National Archives of Canada; and where the record has not been so designated, it shall be destroyed. ***RDA Number:*** 95/009, 96/023, 96/024, 99/006 ***TBS Registration:*** 001001 ***Bank Number:*** CMP PPU 025

Protection of Personnel and Government Property
Description: This bank contains personal information on individuals who have been involved in investigations concerning threats, potential threats, or incidents against persons of national or international importance or involving government property. This bank contains investigational and occurrence reports, statements, and related correspondence as well as personal information on numerous individuals the RCMP has an obligation to protect. In addition to the requirements indicated on the Personal Information Request Form, individuals must provide their full name, date of birth and the geographic location where the information search is to be conducted. ***Class of Individuals:*** The information relates to any person considered a threat or possible threat and victims of threats or possible threats. ***Purpose:*** This information was compiled to assess whether or not given individuals pose a threat or are victims of threats as well as for the purposes of administration and enforcement of the law and detection and prevention of crime. ***Consistent Uses:*** This information is used by domestic and foreign law enforcement agencies in the administration and enforcement of the law and in the detection and prevention of crime. It is used by federal department security officers for security and reliability screening. It is also used for research, planning, evaluation and statistical purposes. This information may be matched with information from other personal information banks and/or program records. All linkages for the purpose of administration or enforcement of the law and in the detection, prevention or suppression of crime are in compliance with the provisions of the Privacy Act. ***Retention and Disposal Standards:*** Records within this bank are retained for a minimum of five calendar years. Where the record has been designated as having

archival or historical value, the record shall be transferred to the control of the National Archives of Canada; and where the record has not been so designated, it shall be destroyed. ***RDA Number:*** 69/123, 95/009, 96023, 96/024 ***Related to PR#:*** CMP PRO 155 ***TBS Registration:*** 001006 ***Bank Number:*** CMP PPU 055

♦ Departmental Security

Security/Reliability Screening Records

Description: This bank contains personal data about individuals who have been the subject of a security clearance or basic or enhanced reliability check while members or employees of the RCMP, or while applying to become a member or employee of the RCMP or individuals employed under contracts awarded or administered by the RCMP. Security clearances are carried out to assess an individual's loyalty and reliability as it relates to loyalty. Reliability checks are done to assess an individual's reliability. The data in the bank would include personal information about the subject and his or her immediate family. It may also include results or criminal records name or fingerprint checks, credit bureau checks, investigative reports related to interviews with neighbours, previous employers, character references, and an analysis of the information. Also on file is the level of security clearance issued or reliability status granted or the reasons same was denied or revoked. ***Class of Individuals:*** Members or employees of the RCMP or individuals applying to become a member or employee of the RCMP or individuals employed under contracts awarded or administered by the RCMP. ***Purpose:*** To assess an individual's loyalty and reliability as it relates to loyalty. Reliability checks are done to assess an individual's reliability. ***Consistent Uses:*** This information is used by accredited domestic and foreign law enforcement and investigative agencies in the administration or enforcement of the law and in the detection, prevention or suppression of crime. This information may be matched with information from other personal information banks and/or classes of records. All linkages for the purpose of administration or enforcement of the law and in the detection, prevention or suppression of crime are in compliance with the provisions of the Privacy Act. ***Retention and Disposal Standards:*** The retention and disposal schedule for these records is 7 years for a Top Secret clearance only and 12 years for Secret, Confidential, Enhanced and Basic clearance from issue date of clearance or security update or 2 years from date of last correspondence on file, whichever is longer. ***RDA Number:*** 95/009, 96/023, 98/001 ***TBS Registration:*** 003208 ***Bank Number:*** CMP PPU 065

♦ Immigration & Passport

Lost or Stolen Passports

Description: This bank contains personal information about individuals who have lost their passports or who have had their passports stolen. Information contained in this bank is provided by and is a copy of the Department of Foreign Affairs and International Trade Passport Office file. In addition to the requirements indicated on the Personal Information Request Form, individuals must provide their full name, date and place of birth and passport number if known. Individuals wishing to access only specific information should identify the material desired, to expedite the processing of their requests. Information in this bank may be maintained in hard copy files as well as in automated form in the Canadian Police Information Centre (CPIC). ***Class of Individuals:*** Individuals who have lost passports or had them stolen. ***Purpose:*** To locate lost or stolen passports and prevent their illegal use. ***Consistent Uses:*** This information is used by domestic and foreign law enforcement and investigative agencies of federal, provincial/state and municipal governments to recover lost or stolen passports and to identify the illegal use of these documents. This information may be matched with information from other personal information banks and/or program records. All linkages for the purpose of administration or enforcement of the law and in the detection, prevention or suppression of crime are in compliance with the provisions of the Privacy Act. ***Retention and Disposal Standards:*** Information is retained until the passport has been located or has expired. Where the record has been designated as having archival or historical value, the record shall be transferred to the control of the National Archives of Canada; and where the record has not been so designated, it shall be destroyed. ***RDA Number:*** 69/123, 95/009, 96/010, 96/023, 96/024 ***Related to PR#:*** CMP IDD 115 ***TBS Registration:*** 001004 ***Bank Number:*** CMP PPU 040

Operational Case Records

Description: This bank contains personal information on individuals who have been involved in investigations under the Criminal Code, federal and provincial statutes, municipal bylaws and territorial ordinances. This bank contains investigational and occurrence reports, statements, exhibit reports, copies of court documents such as summonses, warrants, etc., court briefs, and in some instances records relating to criminal histories. In addition to the requirements indicated on the Personal Information Request Form, individuals must provide their full name, date of birth and the location where the investigation occurred. Individuals wishing to access only specified information should identify the material desired to expedite the processing of their requests. Information in this bank may be maintained in hard copy files as well as in automated form such as the Canadian Police Information Centre (CPIC), Police Information Retrieval System (PIRS), Police Reporting Occurrence System (PROS), Division Information Bank (DIB), and the Missing Children's Registry (MCR). ***Class of***

Individuals: Individuals involved in or the subject of criminal investigations. ***Purpose:*** Compiled in the administration or enforcement of the law and in the detection, prevention, or suppression of crime generally. The social insurance number (SIN) is used only for the following purposes: to establish the accurate identification of an individual; to aid in the identification of a deceased person and locate their next-of-kin; or to identify and locate the owner of lost or stolen property that has a SIN inscribed. ***Consistent Uses:*** This information is used by accredited domestic and foreign law enforcement and investigative agencies, departments of the Criminal Justice System and Courts in the administration or enforcement of the law and in the detection, prevention, or suppression of crime generally. This information is also used by federal departmental security officers for security and reliability screening. This information may also be used for research, planning, training, evaluation and statistical purposes and may be matched with information from other personal information banks and/or program records. All linkages for the purpose of administration or enforcement of the law and in the detection, prevention or suppression of crime are in compliance with the provisions of the Privacy Act. ***Retention and Disposal Standards:*** Records in this bank are retained for a minimum of two calendar years. Where the record has been designated as having archival or historical value, the record shall be transferred to the control of the National Archives of Canada; and where the record has not been so designated, it shall be destroyed. ***RDA Number:*** 91/015, 95/003, 95/009, 95/011, 96/010, 96/023, 96/024 ***TBS Registration:*** 000997 ***Bank Number:*** CMP PPU 005

♦ International Liaison and Protective Operations Directorate

Indices Checks - For the Protection of Persons of National and International Importance
Description: This bank contains personal information on individuals who have applied for media accreditation or who, by virtue of their employment, will be in close proximity to visiting national or international dignitaries. This bank contains biographical data supplied by individuals and is used to determine their eligibility to obtain media accreditation; and biographical data on individuals who will have access to areas where a visiting national or international dignitary may be. In addition to the requirements on the Personal Information Request Form, individuals must identify details pertaining to the VIP visit such as name of visiting dignitary, dates and location of visit, in order to retrieve and expedite the processing of this request. ***Class of Individuals:*** The information relates to media personnel and technicians, and any person that may be in close proximity to the VIP by virtue of their employment. ***Purpose:*** Purpose is to determine eligibility to obtain media or service accreditation for a specific visit, and to comply with the mandate of Protective Services. ***Consistent Uses:*** This information is used by accredited domestic law enforcement agencies to support decisions as to whether media/service accreditation will be granted. This information may be matched with information from other personal information banks and/or program records. All linkages for the purpose of administration or enforcement of the law and in the detection, prevention or suppression of crime are in compliance with the provisions of the Privacy Act. ***Retention and Disposal Standards:*** Records within this bank are retained for a minimum of five calendar years. Where the record has been designated as having archival or historical value, the record shall be transferred to the control of the National Archives of Canada; and where the record has not been so designated, it shall be destroyed. ***RDA Number:*** 69/123, 95/009, 96/023, 96/024, 98/021 ***TBS Registration:*** 001007 ***Bank Number:*** CMP PPU 060

♦ Public Affairs & Information

Access Request Records
Description: This bank contains personal information on individuals who have previously submitted a Personal Information Request Form and/or an Access to Information Request Form concerning RCMP information banks as well as on individuals who have been the subject of a consultation request from another government institution. It contains previously submitted Personal Information Request Forms, Correction Requests, Access to Information Request Forms, the replies to such requests, appeals and information relating to their processing. When requesting access to this bank, in addition to the requirements indicated on the Personal Information/Access to Information Request Form, individuals must also provide their full name and date of birth. ***Class of Individuals:*** Individuals who have previously submitted Personal Information/Access to Information Request Forms concerning information obtained or prepared by the RCMP. ***Purpose:*** To comply with the Privacy Act and the Access to Information Act, to process Personal Information/Access to Information Request Forms, and for research, planning, evaluation and statistical purposes. ***Consistent Uses:*** The information is used for the processing of Personal Information/Access to Information Request Forms for other RCMP information banks. This information is also used for research, planning, evaluation and statistical purposes. ***Retention and Disposal Standards:*** Records within this bank are retained for two calendar years from the date of the last piece of correspondence. Where the record has been designated as having archival or historical value, the record shall be transferred to the control of the National Archives of Canada; and where the record has not been so designated it shall be destroyed. ***RDA Number:*** 69/123, 96/023 ***TBS Registration:*** 001005 ***Bank Number:*** CMP PPU 045

Information Disclosed to Investigative Bodies
Description: This personal information bank contains a copy of the written access request or Treasury Board form 350-56(83/2): Request for Disclosure to Federal Investigative Bodies, forwarded by investigative bodies listed in Schedule II of the Privacy Act to the RCMP under paragraph 8(2)(e). This bank also contains the replies to such requests and particulars concerning information related to their processing. In addition to the requirements indicated on the Personal Information Request Form, individuals must provide their full name and date of birth. ***Class of Individuals:*** Individuals who have been involved in investigations under the Criminal Code, federal and provincial statutes and municipal bylaws are included in this bank. ***Purpose:*** This information was compiled to comply with the Privacy Act, to enable RCMP to account for the number of requests under paragraph 8(2)(e) of the Privacy Act. ***Consistent Uses:*** This information will allow the Privacy Commissioner to audit the procedures utilized as set out in Treasury Board Guidelines 3.7.5. This information is used to verify the conditions of disclosure to federal law enforcement bodies under paragraph 8(2)(e) of the Privacy Act and to account to the Privacy Commissioner for the number of access requests received annually under the Privacy Act. ***Retention and Disposal Standards:*** Personal information in this bank will be kept for two years after date of last correspondence. ***RDA Number:*** 96/023 ***TBS Registration:*** 003207 ***Bank Number:*** CMP PPU 050

Manuals

- Administration Manual
- Career Management
- CPIC Reference Manual
- Financial Management
- Firearms Training
- Forensic Identification
- Health Services
- Informatics
- Laboratory Services
- Operational Manual
- Pay Procedures
- Property Management
- Protective Policing
- Tactical Operations
- Training
- Uniform and Dress

Additional Information

Please see the INTRODUCTION to this publication for information on access procedures under the provisions of the Access to Information Act and the Privacy Act.

Requests for further information about the RCMP and its various programs and functions may be directed to:

Royal Canadian Mounted Police
Public Affairs Directorate
1200 Vanier Parkway
Ottawa, Ontario
K1A 0R2

Tel.: (613) 993-1085

Reading Room

In accordance with the Access to Information Act, members of the public may examine the basic and subsidiary manuals governing the administration and operation of the Royal Canadian Mounted Police at:

Ministry of the Solicitor General
340 Laurier Avenue West
Ottawa, Ontario
K1A 0R2

(hours 8:00 to 15:00)

Reading room facilities are also available regionally. Individuals who wish to avail themselves of this service must contact the Access to Information and Privacy Coordinator to set an appointment.

Canadian Security Intelligence Service

Chapter 40

General Information

Background

The Canadian Security Intelligence Service (CSIS) has operated pursuant to the Canadian Security Intelligence Service Act, since its inception in 1984.

Responsibilities

CSIS collects, analyzes and retains information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada, and reports to and advises the Government of Canada in relation to these matters.

The Service also plays a role in providing security assessments to departments of the Government of Canada (in accordance with section 13 of the CSIS Act and government security policy) and may provide security assessments to the government of a province or any department thereof, any police force in a province, and to the government of a foreign state or institution thereof or an international organization of states or institutions thereof when a security clearance is a required condition of employment. As well, CSIS may advise any Minister of the Crown on matters relating to the security of Canada, or provide any Minister of the Crown with information relating to security matters or criminal activities that is relevant to the exercise of any power or the performance of any duty or function by that Minister under the Citizenship Act or the Immigration Act. It may also conduct such investigations as are necessary in order to provide security assessments or advice to Ministers. Further, CSIS may, in relation to the defence of Canada or the conduct of international affairs, assist the Minister of National Defence or the Minister of Foreign Affairs and International Trade, within Canada, in the collection of information or intelligence relating to the capabilities, intentions or activities of any foreign state or group of foreign states or any person other than a Canadian citizen or permanent resident, or corporation.

Legislation

- Canadian Security Intelligence Service Act

Organization

The Director, under the direction of the Minister, has the control and management of CSIS and all matters connected therewith. The Assistant Director, Secretariat has the responsibility to support the activities of the Director and senior management. The Assistant Director Corporate has general responsibility for information management, internal security, management services, technical and scientific services. The Deputy Director Operations has responsibility for foreign liaison, human sources, operational support and the regional offices. The Assistant Director Operations reports to the Deputy Director Operations regarding the counter-terrorism, counter-intelligence, security screening, analysis and production programs. The Assistant Director Human Resources has overall responsibility for human resource programs.

Information Holdings

Program Records

Corporate
Description: Information relating to information management, internal security, management services, technical and scientific services. ***Topics:*** Activities relating to policy, planning and coordination of matters prepared for the Director and senior management, including the development and maintenance of CSIS policy manuals, directives and external agreements; activities related to the management of information holdings; activities related to the security of information, personnel, facilities and other classified assets; and activities related to the development of security related equipment. ***Access:*** By subject matter. ***Storage Medium:*** Hardcopy and/or EDP systems. ***Program Record Number:*** SIS DDS 040

Human Resources
Description: Information relating to planning, organizing and coordination of the personnel services program. ***Topics:***Activities relating to recruiting, staffing, classification, training and development, compensation and benefits, staff relations, official languages, employment equity and multiculturalism, career management, health services, employee assistance, occupational safety and health, and the employees' association. ***Access:*** By subject matter. ***Storage Medium:*** Hardcopy, EDP and/or microfiche. ***Program Record Number:*** SIS DDS 050

Operations
Description: Information relating to counter-terrorism and counter-intelligence programs, and regional operational activities in respect to these programs; information relating to the identification and development of the government's operational requirements, the results and evaluations; information relating to intelligence analysis and production, operational support, human sources and the security

screening programs. Public safety is the primary requirement. ***Topics:*** Activities relating to organizations and groups engaged in past, current and projected threats to the security of Canada as defined in the CSIS Act; briefly, activities relating to espionage or sabotage that is against or is detrimental to the interests of Canada; or, activities directed toward or in support of such activity; foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada, and are clandestine or deceptive, or involve a threat to any person; activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state; and, activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of the constitutionally established system of government in Canada. Information relating to disclosures of information to authorized recipients under Section 19 of the CSIS Act, including the coordination of CSIS responses to government institutions requesting assistance in preparing threat or risk assessments; activities relating to the maintenance of overall control and accountability for special operations involving the execution of powers under a federal court warrant; activities relating to the management of human sources; activities supporting the government's security clearance program, and activities supporting the government's citizenship and immigration programs and various security programs of provincial governments and agencies. ***Access:*** By subject matter. ***Storage Medium:*** Hardcopy, microfiche and/or EDP systems. ***Program Record Number:*** SIS DDS 010

Secretariat
Description: Information relating to legislative affairs, ministerial relations and Parliamentary liaison, internal review committees, communications, and the Access to Information and Privacy Act (ATIP) program. ***Topics:*** Activities relating to liaison with the Security Intelligence Review Committee, the Office of the Inspector General, Parliamentary committees or commissions, the target authority and warrant review committee; CSIS meetings held internally, interdepartmentally and internationally; ministerial correspondence, including housebook cards; media and public relations; disclosures/policy related to the administration of the ATIP program. ***Access:*** By subject matter. ***Storage Medium:*** Hardcopy and/or EDP systems. ***Program Record Number:*** SIS DDS 045

Personal Information Banks

Access Request Records
Description: This bank contains personal information on individuals who have submitted a formal request under the Privacy Act or Access to Information Act for access to information originally obtained or prepared by CSIS. Documents include access and correction requests, notations, consultations with other government institutions, third party notices, exemptions, exclusions, disclosures, complaints, documents prepared for Court, and other documents pertaining to the processing of the request. ***Class of Individuals:*** Individuals or authorized agents who have submitted a "Personal Information Request Form" or an "Access to Information Request Form" to a federal or provincial institution. ***Purpose:*** To process Personal Information Request Forms and requests under the Access to Information Act. ***Consistent Uses:*** Personal information may be used for the management of CSIS, research, audit, planning, evaluation and statistical purposes and to meet its legal reporting requirements. ***Retention and Disposal Standards:*** As a requirement of the Privacy Act Regulations, information is retained until all avenues of legal appeal have been exhausted with a minimum retention of two years. ***RDA Number:*** 85/001 ***TBS Registration:*** 001681 ***Bank Number:*** SIS PPU 020

Canadian Security Intelligence Service Investigational Records
Description: This bank contains personal information on identifiable individuals whose activities are suspected of constituting threats to the security of Canada; on identifiable individuals who are or were being managed as confidential sources of information; on identifiable individuals no longer investigated by CSIS but whose activities did constitute threats to the security of Canada and which still meet the collection criteria stipulated in section 12 of the CSIS Act, and on identifiable individuals the investigation of whom relate to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities. Exempt Bank Status: This bank has been designated as an exempt bank by Order-in-Council No.14 (CSIS) dated 26 November 1992. ***Class of Individuals:*** Individuals suspected of espionage or sabotage against Canada or the interests of Canada; individuals involved in foreign influenced activities within or relating to Canada that are clandestine or deceptive or involve a threat to any person; individuals involved in activities within or related to Canada directed toward the use of serious acts of violence to achieve a political objective within Canada or a foreign state; or individuals whose activities are directed toward the unlawful covert undermining, or the overthrow by violence, of the constitutionally established government system in Canada; or any other activities described in the definition of "threats to the security of Canada" at section 2 of the CSIS Act; individuals identified relating to a national security concern, the defence of Canada or the conduct of the international affairs of Canada; and individuals who are confidential sources of information. ***Purpose:*** Collected under

section 12 of the CSIS Act with respect to threats to the security of Canada; under section 15 concerning the collection of information for the purpose of providing advice pursuant to section 14; and under section 16 concerning the collection of information or intelligence relating to the capabilities, intentions or activities of foreign states and certain persons. ***Consistent Uses:*** CSIS may only disclose information it obtains if it does so in accordance with the controls of subsection 19(2) of the CSIS Act. First, it may disclose information for the purposes of the performance of its duties and functions under the CSIS Act or the administration or enforcement of that Act, or as required by any other law. The Service may thus disclose personal information to the Government of Canada, for example, as part of its duty to report, and give advice, thereto in relation to activities suspected of constituting threats to the security of Canada. Secondly, where the information in its possession may be used in the investigation or prosecution of an alleged contravention of the law, or where it relates to the conduct of Canada's international affairs or to the defence of Canada, then it may be disclosed to the appropriate police officials and Attorney General, to the Minister of Foreign Affairs and International Trade and to the Minister of National Defence, respectively. Thirdly, information may be disclosed where, in the opinion of the Minister, disclosure to any Minister of the Crown or person in the Public Service of Canada is essential in the public interest and that interest clearly outweighs any invasion of privacy that could result from the disclosure. Pursuant to section 13 and 14 of the CSIS Act, CSIS may also disclose information in the preparation of a domestic or foreign security assessment, or in providing advice under the Citizenship Act or Immigration Act. Personal information may also be disclosed to the Inspector General and the Security Intelligence Review Committee. Information in this bank may also be used for audit, research, planning, evaluation and statistical purposes. ***Retention and Disposal Standards:*** Information in this bank may be retained from two years to twenty years after the last action, subject to the retention and disposal schedules approved by the National Archivist. When files have been designated as historical, they may be transferred to the custody and control of the National Archives of Canada. ***RDA Number:*** 82/013 ***TBS Registration:*** 002872 ***Bank Number:*** SIS PPU 045

Canadian Security Intelligence Service Records
Description: This bank consists of information on individuals who came to the attention of the former RCMP Security Service while carrying out its responsibilities pertaining to informing the government of national security concerns. This bank may also contain information on individuals who incidentally came to the attention of CSIS as a result of carrying out its mandate under section 12 and/or section 16 of the CSIS Act. This bank may contain information on individuals mentioned in reports related to probable unauthorized disclosure of, or unauthorized access to, classified information or assets. ***Class of Individuals:*** Defectors, human sources or individuals, the nature of whose actions or activities caught the attention of CSIS or of its predecessor, the former RCMP Security Service; individuals suspected of espionage or sabotage against Canada or the interests of Canada; individuals involved in foreign influenced activities within or relating to Canada that were clandestine or deceptive or involved a threat to any person; individuals involved in activities within Canada that were directed toward the use of serious acts of violence to achieve a political objective within Canada or a foreign state; or individuals whose activities that were directed toward the unlawful covert undermining, or the overthrow by violence, of the constitutionally established government system in Canada; individuals, other than Canadians or permanent residents, whose capabilities, intentions or activities regarding the defence of Canada or the conduct of international affairs are inimical to the interests of Canada. ***Purpose:*** Collected or obtained by CSIS or the former RCMP Security Service and retained by CSIS under section 12 concerning threats to the security of Canada or under sections 15 or 16 concerning the collection of information relating to the capabilities, intentions or activities of foreign states and certain persons. ***Consistent Uses:*** CSIS may only disclose information if it does so in accordance with the controls of subsection 19(2) of the CSIS Act. First, it may disclose information for the purposes of the performance of its duties and functions under the CSIS Act or the administration or enforcement of that Act, or as required by any other law. The Service may thus disclose personal information to the Government of Canada, for example, as part of its duty to report and give advice to the government regarding activities suspected of constituting threats to the security of Canada. Secondly, where the information in the Service's possession may be used in the investigation or prosecution of an alleged contravention of the law, or where it relates to the conduct of Canada's international affairs or to the defence of Canada, then the information may be disclosed to the appropriate police officials and to the Attorney General, the Minister of Foreign Affairs and International Trade, and the Minister of National Defence, respectively. Thirdly, information may be disclosed where, in the opinion of the Minister, disclosure to any Minister of the Crown or person in the Public Service of Canada is essential to the public interest, and that interest clearly outweighs any invasion of privacy that could result from the disclosure. Pursuant to sections 13 and 14 of the CSIS Act, CSIS may also disclose information in the preparation of a domestic or foreign security assessment, or in providing advice under the Citizenship Act or the Immigration Act. Information in this bank may also be used to assist provincial governments, foreign and domestic agencies, on request, through agreements established under

section 17 of the CSIS Act. (See Classes of Personal Information at the end of this Chapter) Personal information may also be disclosed to the Inspector General and to the Security Intelligence Review Committee. This bank may be used as a source of information or for linking with other information sources for the purposes of fulfilling CSIS's legislated mandate. This information may also be used for audit, research, planning, evaluation and statistical purposes. ***Retention and Dsposal Standards:*** Information in this bank is under continuous review and files are disposed of in accordance with the retention and disposal schedules approved by the National Archivist. When files have been designated as historical, they may be transferred to the custody and control of the National Archives of Canada. ***RDA Number:*** 82/013 ***TBS Registration:*** 000837 ***Bank Number:*** SIS PPU 015

Complaints Against CSIS or Its Employees
Description: This bank contains complaints communicated to CSIS, the Security Intelligence Review Committee (SIRC) or the Office of the Solicitor General of Canada against CSIS or its employees, and any record generated to resolve such complaints that is under CSIS control. In addition to the requirements indicated on the Personal Information Request form, individuals must provide the location where the complaint was reported and the nature of the complaint to retrieve the information of interest for processing. ***Class of Individuals:*** Individuals involved in complaints against CSIS or its employees. ***Purpose:*** To determine the validity of complaints and to record any corrective measures taken, including recommendations for disciplinary or misconduct proceedings. ***Consistent Uses:*** Used in disciplinary and misconduct processes under the CSIS Act. The SIRC or the Inspector General may also use information in this bank to conduct investigations of CSIS. Information in this bank may also be used for the management of CSIS, research, audit, planning, evaluation and statistical purposes. ***Retention and Disposal Standards:*** A minimum of twelve years after the last documentation on the individual complaint file, then transferred to the National Archives of Canada. ***TBS Registration:*** 002762 ***Bank Number:*** SIS PPU 035

CSIS Candidates
Description: This personal information bank contains recruitment documents or applications for employment with CSIS and any related correspondence. This bank may also contain personnel or staffing interviews, polygraph tests, psychological tests, test results, analysts' reports and security assessment advice. Please note that disclosure of psychological and polygraph tests are achieved through your personal examination of the test(s) in the presence of a designated practitioner. Instructions on how to contact the designated practitioner will be issued during the access request process, unless you specify that you do not want access to one or either of the tests. ***Class of Individuals:*** Potential CSIS candidates. ***Purpose:*** To meet the administrative and/or operational needs of CSIS. ***Consistent Uses:*** Information may be transferred to an employee bank if the individual is offered and accepts employment. The candidate's skills may be assessed and, if deemed suitable, may be invited to serve in a capacity other than the position or level of initial interest. Some information in this bank may be used to verify attempts to infiltrate CSIS. This information may also be used for research, audit, planning, evaluation and statistical purposes. ***Retention and Disposal Standards:*** Retained a minimum of two years. However, unsolicited applications are destroyed after six months. ***RDA Number:*** 78/001 ***TBS Registration:*** 000839 ***Bank Number:*** SIS PPU 025

Post Contract Evaluation
Description: This bank contains information relating to suppliers providing a variety of goods and services including EDP hardware, software and consulting support; technical equipment; general property management. This bank contains names, addresses, telephone numbers, supplier capabilities, and post contract evaluations that include quality of goods and services, timeliness, management, security and safety in contract performance. ***Class of Individuals:*** Suppliers of goods and services. ***Purpose:*** To determine whether or not to consider suppliers of goods and services for a potential contract. ***Consistent Uses:*** This information is used to evaluate supplier's contract performance for the purpose of determining whether or not to consider certain suppliers for the provision of goods and/or services. Information in this bank may also be used as a source of information in respect to the CSIS 'Self Protection Activity' bank or the 'Security and Integrity of Government Property, Personnel and Assets' bank. ***Retention and Disposal Standards:*** The records in this bank are retained for a period of six years, and then disposed of in accordance with the schedule approved by the National Archivist. ***RDA Number:*** 86/001 ***TBS Registration:*** 004036 ***Bank Number:*** SIS PPU 060

Security and Integrity of Government Property, Personnel and Assets
Description: This bank contains personal information on individuals in contact with CSIS whose actions have raised concern about the security and integrity of government property, personnel or assets. This bank may contain letters, notes, facsimile copies, contact reports and related correspondence, and access control data or examination results of telephone use that has been used in a decision-making process. ***Class of Individuals:*** Individuals of concern regarding the security and integrity of government property, personnel or assets and CSIS employees who were the object of such actions. ***Purpose:*** This information was

compiled as an aid to internal security investigations of alleged breaches of security or in relation to the safety and integrity of government property, personnel and assets. ***Consistent Uses:*** Information may be disclosed to the accredited police agency having local jurisdiction of an incident. Information in this bank may be matched with information from other CSIS personal information banks for the purpose of preserving the security of Canada or CSIS internal security. ***Retention and Disposal Standards:*** The records in this bank are retained for a period of five years, ten years for access control data, and then disposed of in accordance with the schedule approved by the National Archivist. ***TBS Registration:*** 003632 ***Bank Number:*** SIS PPU 055

Security Assessments/Advice
Description: This bank contains personal information on individuals who are or have been the subject of a request for a security assessment for pre-employment/employment with federal or provincial government departments and agencies and the private sector working under federal government contracts, when a security clearance is a required condition of employment. This includes information obtained during internal quality control investigations. Similar records are held in respect to security assessments required by a provincial government, a foreign state, or an international organization of states. This bank may also contain criminal records, credit bureau results, security analyses, security assessments and investigative reports, related correspondence and a notation of the level of security clearance granted. In addition, this bank may hold information on persons subject to security assessment or advice relative to the Citizenship Act or Immigration Act. ***Class of Individuals:*** Persons for whom CSIS was asked to provide a security assessment or advice for pre-employment/employment, including contract and company personnel working under federal or provincial government or agency contracts; CSIS and CF/DND employees; individuals requiring access to internationally protected persons, VIPs and special events; the Parliamentary Precinct and the restricted areas of airports; individuals who would seek admittance or to remain lawfully in Canada; and individuals seeking citizenship. By virtue of the screening process, personal information may be held on individuals who are not themselves the subject of the security assessment. ***Purpose:*** Collected under section 15 of the CSIS Act to provide security assessments pursuant to section 13 or advice pursuant to section 14 of the Act. ***Consistent Uses:*** Pursuant to sections 19(2), 13 and 14 of the CSIS Act, CSIS may disclose information or may match information in the preparation of a domestic or foreign security assessment or in providing advice pertinent to the Citizenship Act or Immigration Act or where the information relates to the conduct of the international affairs of Canada, to the Secretary of State for External Affairs, or where the information is relevant to the defence of Canada, to the Minister of National Defence. It may also be used for data matching, or for the purposes of conducting lawful investigations in matters which may on reasonable grounds, be suspected of constituting threats to the security of Canada and in other lawful investigations. In addition, information may be provided to the Inspector General and the Security Intelligence Review Committee, the Federal Court and the Supreme Court. This information may also be used for research, audit, planning, evaluation and statistical purposes. ***Retention and Disposal Standards:*** Information in this bank may be retained from two years to twelve years from the last updating, and then disposed of subject to the Retention and Disposal schedules approved by the National Archivist. When files have been designated as historical, they may be transferred to the custody and control of the National Archives of Canada. ***RDA Number:*** 82/013 ***TBS Registration:*** 000835 ***Bank Number:*** SIS PPU 005

Self Protection Activity
Description: This bank contains personal information on individuals in contact with CSIS with a view of providing services directly or through contract to CSIS. The information may include the individual's name, any aliases and other personal identifiers. Under subsection 16(2) of the Privacy Act, CSIS consistently responds to all applicants in a manner that neither confirms nor denies the existence of personal information in this bank, regardless of whether or not personal information about the applicant exists in this bank. ***Class of Individuals:*** Individuals in contact with the Service. ***Purpose:*** The purposes for which the information in this bank was recorded is in support of CSIS's counter intelligence program. The information will allow CSIS to better protect itself from infiltration by hostile foreign services and others whose interests are inimical to the interests of Canada. ***Consistent Uses:*** Information in this bank may be used in support of CSIS's counter intelligence program. Information in this bank may also be used for audit purposes. ***Retention and Disposal Standards:*** Information in this bank will be retained for a minimum of ten years, and destroyed when considered to be of no further value. **Related to:** SIS DDS 010 ***TBS Registration:*** 003297 ***Bank Number:*** SIS PPU 050

Classes of Personal Information

In the course of carrying out the daily investigative activities and functions of the Canadian Security Intelligence Service, personal information may be accumulated such as in the security assessments and crisis management programs which are not described in the specific personal information banks. This information is not used for an administrative purpose affecting an individual, and can include names, addresses and other identifying data in a record. Such

information is only retrievable if full specifics are provided concerning the subject matter. The retention period for this form of information is in accordance with the retention and disposal schedules approved by the National Archivist.

Unsolicited opinions or requests for information are received by the Service. This information is not used for an administrative purpose, other than to respond in some instances to the originator. This correspondence is stored in a file associated with the subject matter, and is disposed of in a manner authorized by the National Archivist.

Some interview clips on video cassettes purchased from the Public Service Commission are being used to help English and French speaking CSIS employees to prepare for oral interaction tests conducted as an administrative measure in support of the CSIS official languages program. The personal information in the cassettes is not being used for an administrative purpose respecting any of the individuals presented in the videos.

Under the National Archives Act, index cards, registers and automated ledgers and indices are required to be created on all files opened by the Service since its inception. They contain general information such as the file numbers, titles, file creation and disposition dates. These personal information holdings serve as an information management tool that is created and used to account for the opening and disposition of each file. The index cards and registers are retained for a period of time after the disposition of the information holdings itself. An individual wishing access to the general information about themself that may be contained in the index cards and registers is required to provide the file number or sufficiently specific information as to render it reasonably retrievable.

Manuals

- Administration Manual
- Human Resources Manual
- Immigration Screening Profiles Manual
- Operational Manual
- Security Policy Manual
- Security Screening Procedures Manual

Additional Information

Please see the INTRODUCTION to this publication for information on access procedures under the provisions of the Access to Information Act and the Privacy Act.

Date and place of birth must be included in any request made under the Privacy Act to verify that it is you, and not someone else, asking for the information.

Reading Room

The Solicitor General's reading room contains records supplied by CSIS under the Access to Information Act. The address is:

Access to Information and Privacy Co-ordinator
Solicitor General Canada
Sir Wilfrid Laurier Building
1st Floor, 340 Laurier Avenue West
Ottawa, Ontario
K1A 0P8

Appendix "C"

Relevant Statutory Provisions

The purposes of the FOIPP ACT are set out in section 2 as follows:

> 2 (1) The purposes of this Act are to make public bodies more accountable to the public and to *protect personal privacy* by
>
> (a) giving the public a right of access to records,
>
> (b) giving individuals a right of access to, and a right to request correction of, personal information about themselves,
>
> (c) specifying limited exceptions to the rights of access,
>
> (d) *preventing the unauthorized collection, use or disclosure of personal information by public bodies*, and
>
> (e) *providing for an independent review of decisions made under this THE FOIPP ACT.*
>
> (2) This Act does not replace other procedures for access to information or limit in any way access to information that is not personal information and is available to the public. *(emphasis added)*

Section 3 of the FOIPP ACT deals with the scope of that Act. That section reads, in part;

> 3 (1) This Act applies to all records in the custody or under the control of a public body, including court administration records, but does not apply to the following:
>
> ...
>
> (2) This Act does not limit the information available by law to a party to a proceeding.

"Public body" is defined under the FOIPP ACT as meaning;

> (a) a ministry of the government of British Columbia,
>
> (b) an agency, board, commission, corporation, office or other body designated in, or added by regulation to, Schedule 2, or
>
> (c) a local public body.

The FOIPP ACT defines "personal information" as meaning "recorded information about an identifiable individual".

Section 30 of the FOIPP ACT deals with a public body's obligations concerning the security of the personal information within its custody or control. That section reads as follows:

"The head of a public body must protect personal information in the custody or under the control of the public body by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal."

Section 33 of the FOIPP ACT provides as follows:

A public body must ensure that personal information in its custody or under its control is disclosed only

(a) in accordance with Part 2,

(b) if the individual the information is about has identified the information and consented, in the prescribed manner, to its disclosure,

(c) for the purpose for which it was obtained or compiled or for a use consistent with that purpose (see section 34),

(d) in accordance with an enactment of British Columbia or Canada that authorizes or requires its disclosure,

(d.1) in accordance with a provision of a treaty, arrangement or agreement that

(i) authorizes or requires its disclosure, and

(ii) is made under an enactment of British Columbia or Canada,

(e) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information,

(f) to an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer, employee or minister,

(f.1) to an officer or employee of a public body or to a minister, if the information is necessary for the delivery of a common or integrated program or activity and for the performance of the duties of the officer or employee or minister to whom the information is disclosed,

(g) to the Attorney General for use in civil proceedings involving the government,

(h) to the Attorney General or a person referred to in section 36 of the *Coroners Act*, for the purposes of that Act,

(i) for the purpose of

(i) collecting a debt or fine owing by an individual to the government of British Columbia or to a public body, or

(ii) making a payment owing by the government of British Columbia or by a public body to an individual,

(j) to the auditor general or any other prescribed person or body for audit purposes,

(k) to a member of the Legislative Assembly who has been requested by the individual the information is about to assist in resolving a problem,

(l) to a representative of the bargaining agent who has been authorized in writing by the employee, whom the information is about, to make an inquiry,

(m) to the archives of the government of British Columbia or the archives of a public body, for archival purposes,

(n) to a public body or a law enforcement agency in Canada to assist in an investigation

(i) undertaken with a view to a law enforcement proceeding, or

(ii) from which a law enforcement proceeding is likely to result,

(o) if the public body is a law enforcement agency and the information is disclosed

(i) to another law enforcement agency in Canada, or

(ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority,

(p) if the head of the public body determines that compelling circumstances exist that affect anyone's health or safety and if notice of disclosure is mailed to the last known address of the individual the information is about,

(q) so that the next of kin or a friend of an injured, ill or deceased individual may be contacted, or

(r) accordance with sections 35 and 36.

Appendix "D"

U.S. Department of Justice

Civil Division

May 19, 2004

By Federal Express

Honorable Denise Page Hood
United States District Judge
Eastern District of Michigan
Theodore Levin United States Courthouse
231 W. Lafayette Boulevard
Detroit, Michigan 48226

Re: Muslim Community Association of Ann Arbor, et al., v. Ashcroft, et al., Civil No. 03-72913 (E.D. Mich.)

Dear Judge Hood:

Defendants filed their motion to dismiss this action on October 3, 2003, together with a declaration executed by James A. Baker, Counsel for Intelligence Policy, United States Department of Justice ("Baker Declar."). As stated in paragraph 3 of Mr. Baker's declaration, on or about September 18, 2003, the Attorney General declassified the number of times that the Department of Justice, including the Federal Bureau of Investigation (FBI), has utilized Section 215 of the USA PATRIOT Act (which is the subject of plaintiffs' challenge in this action). During the period between October 26, 2001 and September 18, 2003, the Department, including the FBI, presented no applications to the Foreign Intelligence Surveillance Court ("FISA Court") for issuance of an order authorized by Section 215. Baker Declar., ¶ 3. The Attorney General's declassification determination applied only to the number of times Section 215 had been used up to the date of his decision (*i.e.*, September 18, 2003). Similarly, Mr. Baker's testimony regarding the use of Section 215 pertains solely to the period identified in his declaration, which encompasses the entire period covered by the factual allegations in plaintiffs' complaint in this action. As defendants emphasized in the memorandum filed in support of their motion to dismiss, "the Government may use this provision under appropriate circumstances in the future . . . ." Memorandum in Support of Defendants' Motion to Dismiss, at 1.

The purpose of this letter is to advise the Court that, pursuant to 50 U.S.C. § 1862(b), on or before June 30, 2004, the Department of Justice expects to submit to the judiciary committees of the United States Senate and the U.S. House of Representatives a biennial report that will contain information regarding Section 215 applications, if any, submitted during the period July 1, 2003 to December 31, 2003. Thus, the report will include a three and a half month period that is not addressed

in Mr. Baker's declaration (*i.e.*, from September 19, 2003 to December 31, 2003). Because plaintiffs' complaint was filed before the latter period commenced, any Section 215 applications that might have been submitted during that three and one half month period fall outside of the time period encompassed by plaintiffs' factual allegations in this action.

The information contained in the report is to be submitted to the committees in classified form, and is not subject to public release. *See American Civil Liberties Union v. United States Department of Justice*, Civil Action No. 03-2522 ESH (D.D.C. May 10, 2004), slip op., at 2-3, 21 (copy attached). Given the unique need for confidentiality in the context of foreign intelligence investigations, the Government is simply not in a position to undertake an obligation to keep the Court or the plaintiffs informed on an ongoing basis if and when the Government seeks a Section 215 Order from the Foreign Intelligence Surveillance Court. Nevertheless, as the Government has explained, the recipients of any Section 215 orders will have a full and fair opportunity to present any constitutional objections to the orders before the issuing FISA court.

To ensure that the public record relating to the proceedings before this Court is complete, defendants are filing a copy of this letter with the Court's clerk. Should the Court require any further information with respect to these matters, upon request by the Court, defendants will endeavor to provide it in a form and manner appropriately tailored to the nature and classification level of the information needed.

Respectfully submitted,

Joseph W. LoBue
Senior Trial Counsel

Enclosure

cc: All Counsel

Appendix "E"

The following are specific mitigation strategies that are contemplated by the Province. Each ASD initiative will be assessed and appropriate strategies applied. They will vary from initiative to initiative.

(a) Technology and Business Processes

(i) clearly identifying and segregating personal information;

(ii) limiting access, such as through logical security measures (including passwords, IDs and similar measures) and physical security;

(iii) restrictions on the issuance of passwords (including the Province potentially being involved in that process);

(iv) audit and control procedures to ensure that measures continue to effectively limit access to the personal information;

(v) tracing and audit trails for data access, including access logs;

(vi) to the extent reasonably possible, automatic notification processes (either in all cases or in certain limited circumstances such as irregular or large scale access) with notification likely going to Province employee);

(vii) restrictions on data mobility, including restricting data from leaving British Columbia premises in both physical and electronic formats (e.g. email filtering, restricting mobile storage devices and limiting remote access);

(viii) ensure that the Province's security requirements (including the requirements of the *FOIPP Act* and the security requirements prescribed by the Office of the Chief Information Officer for the Province of BC and in chapter 12 of the Province's CORE Manual) are met by the service provider;;

(ix) strong technology security measures including firewalls and encryption;

(x) permit access to personal information only by personnel who require it in order to perform their duties;

(xi) adopting recommendations of the Commissioner, as found in the "Guidelines for Data Service Contracts", OIPC Guideline 01-02, (attached as Appendix "H"), as appropriate;

(xii) include detailed privacy and security standards in each contract;

(xiii) dedicated compliance officer who monitors processes;

(xiv) complete a detailed Privacy Impact Assessment before any decision is made to outsource government services or where material changes are made to those services after they have been outsourced; and

(xv) require the adoption of privacy enhancing technologies to improve security and restrict access to information to authorized users.

(b) Employee Strategies

(xvi) direct agreements between the Province and employees which include non-disclosure obligations and obligation to advise the Province in the event that the employee becomes aware of any potential disclosure;

(xvii) requirement that the service provider make certain commitments to its employees, specifically that the Province/employee agreement takes precedence and the service provider agreeing that there would not be adverse consequences to the employee for compliance with the Province/employee agreement;

(xviii) ensuring that the service provider's employees receive appropriate training regarding the applicable processes and rules relating to access to and control of government information. For example, employees should receive training regarding what levels of access are permitted in respect of government information, in what circumstances may such levels of access be varied, from which individuals may the employee receive instructions regarding such processes, and in what circumstances is the employee obligated to disclose to a supervisor (or external individual) the occurrence of activities that are inconsistent with the contract;

(xix) special security clearance requirements for certain employees;

(xx) reoccurring (perhaps annually):

A. training of employees; and

B. contractual commitment from employees (similar to annual oath) and confirmation from employees that there has been no breach of the Province/employee agreement;

(xxi) for U.S. employees that are in any way involved in providing services:

A. no data access unless absolutely required to perform duties;

B. "dummy" data be used to the extent possible so that people are not working on nor have access to "real data";

C. where reasonably possible utilize Canadian residents to do the work;

D. where U.S. employees must have access to the data, access would only be in British Columbia at the designated facility, with no ability to remove data from the premises, and each such employee signing a direct agreement with the Province;

E. data conversion would be overseen by (or monitored by) Canadian resident that are subject to the Province/employee agreement.

(xxii) hotline established for employees to call with any suspected disclosure of personal information.

(c) Contractual Measures

(xxiii) Require the Canadian service provider to provide notice to the Province of a request by its U.S. affiliate for government information. The confidentially requirements of the *Patriot Act* would not apply to a Canadian or B.C. company;

(xxiv) require personal information to be kept in Canada;

(xxv) expressly prohibit access to personal information by a U.S. affiliate;

(xxvi) require the Canadian service provider to obtain a performance bond that would be triggered upon the disclosure of any personal information to its U.S. affiliate;

(xxvii) the Canadian service provider would agree to pay substantial liquidated damages in the event of any disclosure of personal information;

(xxviii) include termination rights in the outsourcing agreement in the event of any disclosure of personal information; and

(xxix) provide the Province with power of attorney and other contractual rights that allow the Province to take over the operations of the

Canadian service provider in the event of a potential disclosure of personal information.

(xxx) Flow through of provisions to sub-contractors and affiliates of provider.

(d) Corporate Strategies

(xxxi) require that all records containing personal information be in the sole custody of, and may be accessed only by, an entity incorporated in British Columbia (or pursuant to federal legislation)

(xxxii) require that all directors of the Canadian service provider be Canadian citizens and British Columbia resident individuals that sign direct agreements with the Province restricting disclosure and requiring them to advise the Province of any potential disclosure;

(xxxiii) place restrictions in the incorporation documents of the Canadian service provider that make disclosure of personal information pursuant to the *Patriot Act* to be outside of the company's corporate authority;

(xxxiv) establishing a three layer corporate structure with the U.S. company owning the shares of a Canadian holding company which in turn holds the shares of the Canadian service provider, thereby removing direct ownership of the Canadian service provider from the U.S. company;

(xxxv) as a more extreme measure, a trust arrangement might be implemented pursuant to which legal ownership of the shares of the Canadian entity could be vested in either the Province or a third party Canadian trustee while beneficial ownership of the shares is held by the U.S. company. The trust mechanism could be structured so that the beneficial owner has no authority to compel the Canadian entity to disclose personal information.

Appendix "F"

HBO – Privacy and Security Mitigation Strategies
July 15, 2004

The Province and MAXIMUS, Inc. ("MAXIMUS U.S.") are in negotiation on the contract for the HBO Project for the provision of services by B.C. based and incorporated service providers (the "Service Provider") who are subsidiaries of MAXIMUS Canada. The following reflect the mitigation strategies that the parties are currently considering.

1. Employees/Contractors

   (a) Direct agreements between the Province and Service Provider employees. These agreements will include non-disclosure obligations and an obligation to advise the Province in the event that the employee becomes aware of any potential disclosure.

   (b) Direct agreements between the Province and all other people who are not Service Provider employees (including MAXIMUS U.S. employees who are involved in the services and employees of suppliers and subcontractors). These agreements would include the same elements as described in (a) above. These agreements will have additional remedies including liquidated damages.

   (c) Requirement that the Service Provider include certain language in its employment agreements with its employees, including precedence of Province/employee agreement over the employment agreement and express agreement by the Service Provider that there would not be adverse consequences to the employee for compliance with Province/employee agreement (whistleblower section).

   (d) Policies and Procedures regarding security and privacy

   (e) Privacy Plan (including protocol in the event of a security or privacy breach)

   (f) Education and training

   (b) Special security clearance requirements for certain employees;

   (c) Annual re-training of employees and contractual commitment from employees (similar to annual oath) and confirmation from employees that there has been no breach of Province/employee agreement;

   (d) for U.S. employees working on transition or transformation:

      (i) no data access unless absolutely required to perform duties;

(ii) "dummy" data be used to the extent possible for the transition and transformation processes so that people are not working on nor have access to "real data";

(iii) where reasonably possible utilize Canadian residents to do the work (or, if possible, train Canadians);

(iv) where U.S. employees must have access to the data, access would only be in British Columbia through employees of the Service Provider at the designated facility, with no ability to remove data from the premises, and each such employee signing the direct agreement with the Province noted above; and

(v) data conversion would be overseen by (or monitored by) Canadian resident that we would be confident would comply with the "whistleblower" provisions.

(e) whistleblower hotline to be set up for employees to report any potential disclosure

(f) designated privacy, security and compliance officer responsible for monitoring and enforcing privacy and security measures and who takes functional direction from the Province (not the Service Provider)

2. Technology and Business Processes

(a) data and all back-ups only to be located in Canada;

(b) annual compliance certificate regarding security and privacy compliance;

(c) records and retention policies that conform to Province requirements;

(d) privacy policy covering issues such as data sharing, FOI requests and investigations;

(e) security audit will be conducted prior to handover;

(f) risk and control reviews will be performed by the Service Provider (to the satisfaction of the Province) prior to implementation of any material business or technology change;

(g) privacy impact assessments including at transition points in order to ensure the security and protection of data;

(h) security policies and standards including ISO17799:2000 (as revised from time to time)

(i) regular audits including SysTrust audits

(j) restrictions to data removal methods including (i) restrictions on outbound web and email access; and (ii) hardware restrictions including limitations on floppy drives, CD ROM burners, USB smartdrives and similar devices;

(k) any offsite storage must be in British Columbia, approved by the Province with the Province having direct confidentiality agreement with the Service Provider;

(l) strong technology security measures including firewalls and encryption;

(m) physical security of data rooms and premises;

(n) segregation of data with restricted access;

(o) tracing and audit trails for data access, including access logs;

3. Contractual

(a) termination rights;

(b) liquidated damages;

(c) bonding/performance guarantee

(d) flow through of obligations to subsidiaries (including direct agreements between the Province and subcontractors and their employees on certain issues)

(e) clear contractual provisions regarding Province ownership and control of the data

(f) detailed confidentiality provisions

(g) ability for the Province to replace Service Provider employees with employees of the Province in certain circumstances

(h) power of attorney granted to the Province to perform certain actions on behalf of the Service Provider in certain circumstances

(i) performance guarantee from MAXIMUS Canada and financial guarantee from MAXIMUS U.S.

4. Corporate Structure

(a) service delivery by two B.C. entities (defined above as the Service Provider)

(b) restrictions to be placed in Articles of the Service Provider that restricts disclosure

(c) directors of the Service Provider to be British Columbia residents who will sign non-disclosure agreements directly with the Province

(d) Shares of Service Provider to be held in trust with MAXIMUS Canada being the beneficial owner. In the event of a risk of disclosure of data and no other options available, beneficial interest and full control of the Service Provider transferred to the Province.

(e) MAXIMUS Canada and MAXIMUS U.S. subject to contractual restrictions with the Province regarding disclosure of data

Appendix "G"

Scenarios – Under *Patriot Act* - FBI Serve MAXIMUS U.S. With Order To Access Data

Options available to MAXIMUS U.S.:

1. **MAXIMUS U.S. employees directly access data held in U.S.**

   - Mitigation measures:
     - No data held in U.S. and data may not be exported to U.S.
     - Employees of MAXIMUS U.S prohibited from accessing data held in Canada*

2. **MAXIMUS U.S. officials remotely access data held within Canada**

   - Mitigation measures:
     - No remote access from outside Canada
     - Employees of MAXIMUS U.S. prohibited from accessing data held in Canada*

3. **MAXIMUS US orders MAXIMUS Canada employees to access data held by B.C. service provider (the "Service Provider"):**

   - Mitigation measures:
     - Data segregated so that only Service Provider has access (MAXIMUS Canada, MAXIMUS US and their employees do not have access)*
     - MAXIMUS Canada, which is governed by Canadian law, has contractually agreed with Province that it will not disclose and it will advise the Province if it is requested to disclose data
     - MAXIMUS Canada unable to compel Service Provider to disclose due to trust structure and contractual restrictions on the Service Provider

4. **MAXIMUS US orders an employee of the Service Provider with access to data to release data:**

   - Mitigation measures:
     - All employees of Service Provider sign non-disclosure agreements directly with the Province. Non disclosure agreement includes requirement for the employee to notify Province in the event he/she becomes aware of any potential disclosure
     - Employment agreements between Service Provider and its employees must state that the non-disclosure agreement with the Province has precedence over employment agreement and that management has no authority to instruct employees to act contrary.

- Potential damages through litigation and termination of employment for breach of non-disclosure agreement
- Whistle blower protection for all staff in Service Provider including hotline that they are encouraged by Service Provider to use in the event that they are requested to disclose data
- Electronic tools monitor and trace unusual access or copying of data
- Restrictions on ability to remove data from the B.C. service centre
- Dedicated privacy and security officer monitors compliance
- Service Provider, MAXIMUS Canada and MAXIMUS U.S. all face significant financial penalty and contract termination
- Training of employees required. Training emphasizes that employees' primary obligation under non-disclosure agreement with Province, that there are no adverse consequences for adhering to Province non-disclosure agreement, that there is a hotline to report potential disclosures and that there are serious consequences for disclosing data.

Overriding all of these scenarios, a privacy breach if detected would trigger trust mechanism – ownership of Service Provider would revert to the Province.

*Contract would permit the Province to grant a MAXIMUS U.S. employee the opportunity to view personal information for the purposes of transition activity or implementation of technology; however such viewing would be limited to the B.C. operating centre, supervised by Canadians, with no ability on the part of that U.S. employee to move or disclose the information or the medium on which it is stored, and the information would, where possible, be stripped of personal identifiers.

Appendix "H"

Health Benefit Operations: Summary of Privacy and Security Provisions

The following table summarizes privacy and security measures in the context what is currently in place for contracted MSP and PharmaCare services and the proposed environment with Maximus as the service provider.

Mitigation Strategy / Contract Provisions (✗ = not a specific requirement; ✓ = specific requirement)	Current Contracts	Draft MAXIMUS Contract
• Service provider policies and procedures outline all privacy and security objectives, methodologies, and disclosure requirements;	✓	✓
• Within the BC service provider, access will be further segregated to align with specific job requirements;	✓	✓
• Tools will be implemented to enable trace and audit of all data access/copying, including individual user logs;	✓	✓
• Strong technology security measures will be implemented, including firewalls, encryption and physical security;	✓	✓
• Strict records management and retention policies will be implemented;	✓	✓
• Privacy Impact Assessments will be required prior to any systems change;	✓	✓
• Contract includes termination rights in the event of disclosure or privacy breach;	✓	✓
• Province has power of attorney and other contractual rights that allow the Province to take over the operations of the BC Entity in the event of a potential disclosure of personal information	✗	✓
• Separate BC Entity held in trust structure – all Canadian resident Directors on Board of BC Entity	✗	✓
• All employees and sub-contractors who have access to HBO data sign non-disclosure agreements with the Province;	✗	✓
• Non-disclosure agreements include the requirement for the signer to notify the Province in the event that he/she becomes aware of any potential disclosure;	✗	✓
• The service provider agreements with its own employees must state that the employee non-disclosure agreement with the Province has precedence over its employment agreement; and will include "whistleblower" protection;	✗	✓

Mitigation Strategy / Contract Provisions (✗ = not a specific requirement; ✓ = specific requirement)	Current Contracts	Draft MAXIMUS Contract
• Whistleblower hotline for employees to call	✗	✓
• The service provider will require annual confidentiality commitments from all employees	✗	✓
• A detailed Privacy Plan will be created and referenced in the contract;	✗	✓
• Special restrictions on data access and oversight/supervision requirements apply to US employees working on transition and transformation activities.	✗	✓
• Data storage and access, including remote access, will be only in Canada, and can only be changed with the Province's express consent;	✗	✓
• Data access will be segregated so that only the BC service provider (and not the Canadian or US parents) has access;	✗	✓
• Outbound web and email access for staff will be prohibited or restricted, except as required to deliver specific services;	✗	✓
• Hardware that would enable data to be copied and taken off site, such as removable floppy drives, CD burners and USB smart drives will be restricted to designated personnel;	✗	✓
• service provider must have dedicated Privacy and Security Officer who monitors compliance;	✗	✓
• Contract includes liquidated damages in the event of disclosure or privacy breach in response to a requirement of a foreign country.	✗	✓

Appendix "I"

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

GUIDELINES FOR DATA SERVICES CONTRACTS

OIPC GUIDELINE 01-02

Date: May 8, 2003
(Replaces: November 14, 2001)

1.0 PURPOSE OF THIS DOCUMENT

These guidelines of the Office of the Information and Privacy Commissioner for British Columbia ("OIPC") are for use by public bodies, including any provincial government ministries, that contract out:

- the processing or storage of information that includes personal information;
- the operation or management of computerized systems containing personal information; or
- services involving the collection, use or disclosure of personal information.

Despite the possible cost-savings or other benefits of contracting out such information services, public bodies must not forget the risks to privacy that can arise where personal information is being collected, used, disclosed or managed by an outside service provider who is not familiar with, or equipped to meet, the statutory obligations regarding personal information in Part 3 of the *Freedom of Information and Protection of Privacy Act* ("Act"). (A copy of the Act is found at www.oipc.bc.ca/legislation/FOI-ACT.pdf.) Privacy risks include use or disclosure of personal information by unauthorized personnel, compromised integrity of personal information, accidental disclosure of personal information, improper use or disclosure of personal information and improper retention or secondary use of personal information. These guidelines are intended to address risks to privacy that may arise in the contracting out situations described above.

These guidelines acknowledge that a public body cannot, by contracting out, relieve itself of its privacy obligations under Part 3 of the Act. To maintain public confidence in the public body's handling of personal information, and to ensure compliance with the Act, each contract for personal information services should require the service provider to comply with the Act and any privacy practices specified in or under the contract. It is also important for the public body to monitor performance, and enforce the agreement, including by conducting periodic audits as provided in the contract.

The OIPC recognizes that implementation of these guidelines will have cost implications for the public body. It is within a public body's discretion to decide which of these guidelines should be implemented in any such arrangement, and how, but it must be remembered that these guidelines will in turn guide the OIPC in assessing any contracting-out arrangement when investigating whether the public body has met its obligations under Part 3 of the Act. For an example of such an investigation, see Investigation Report 01-01, at http://www.oipc.bc.ca/investigations/reports/IR01-01.pdf.

These guidelines have benefitted from study of publications of the Office of the Information and Privacy Commissioner of Ontario, whose efforts are gratefully acknowledged.

This document is for information only. It does not provide legal or other advice. These guidelines do not constitute a decision or finding by the OIPC respecting any matter within the jurisdiction of the Information and Privacy Commissioner under the Act. These guidelines do not affect the powers, duties or functions of the Information and Privacy Commissioner respecting any complaint, investigation or other matter under or connected with the Act and the matters addressed in this document.

2.0 GENERAL

2.1 Definitions – These guidelines deal with contracting out arrangements that involve "personal information" as defined in the Act. The Act defines "personal information" as "recorded information about an identifiable individual". This will *include* the following types of personal information:

(a) the individual's name, address or telephone number,

(b) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,

(c) the individual's age, sex, sexual orientation, marital status or family status,

(d) an identifying number, symbol or other particular assigned to the individual,

(e) the individual's fingerprints, blood type or inheritable characteristics,

(f) information about the individual's health care history, including a physical or mental disability,

(g) information about the individual's educational, financial, criminal or employment history,

(h) anyone else's opinions about the individual, and

(i) the individual's personal views or opinions, except if they are about someone else.

Personal information is "recorded information" *of any kind*, so long as it is "about an identifiable individual". This means that, even if someone's name or other identifier is not part of the personal information, the individual the information is about may be "identifiable", making the information "personal information". If personal information is involved, the public body must comply with Part 3 of the Act in collecting, using, disclosing and securing the personal information and this extends to the contracting-out arrangement.

The Act defines the term "record" as follows:

> **"record"** includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records;

A "record" is *any* physical, electronic or other medium in or on which personal information is recorded. The Act's definition says that a "computer program" is not a

record. This is intended to protect software and does not limit the Act's application to personal information that is in electronic form.

The Act's definitions of personal information and record should be incorporated into any contract for personal information services.

2.2 **Privacy Impact Assessment** – A public body should carry out a privacy impact assessment ("PIA") before it makes the final decision to contract out personal information services. A link to the model PIA tool jointly developed by the OIPC and the Corporate Privacy and Information Access Branch of the Ministry of Management Services is found at http://www.mser.gov.bc.ca/foi_pop/manual/forms/pia.doc. At present, it is mandatory for provincial government ministries to carry out PIAs.

2.3 **Involving Privacy Staff in the Contract Process** – A public body should involve its privacy staff in preparing tender documents or request for proposal ("RFP") documents. Access and privacy staff should also be involved in the actual contract process as well. The RFP or tender documents should make it clear to prospective contractors what the Act requires and should alert them, in as much detail as practicable, to the specific privacy duties and obligations they will be required to meet. This will ensure that bids or proposals address the privacy requirements at the outset. Ideally, a public body that contracts out personal information services frequently should create, and send to prospective service-providers, standard-form privacy provisions for RFPs and contracts.

3.0 GUIDELINES FOR CONTRACT TERMS

Each contract should include provisions addressing the matters discussed below. A public body also should refer to any available sources for current, generally-accepted best practices and consider their implementation through the contract, even if they are not mentioned here.

The complexity of some arrangements may require further provisions than are contemplated by the following guidelines. Some contracts may require fewer controls than the following guidelines contemplate.

Much depends on the circumstances, mainly the nature of the personal information in question and the nature of the services to be provided to the public body. For example, if the personal information is sensitive information (such as health information) and the services will involve collection, use and disclosure of such information (as opposed to simple storage or archiving of information), the service agreement should reflect these guidelines.

In more straightforward cases (such as where the information is not sensitive or the services do not involve collection, use or disclosure of personal information), the service contract may be more basic. Standard-form privacy protection clauses of that kind can be found through the following Ministry of Management Services website: <http://www.mser.gov.bc.ca/FOI_POP/PPS/default.htm>. That website contains links to

a privacy protection contract schedule designed for provincial government ministries and a schedule designed for use by other public bodies.

3.1 General Provisions About Application of the Act – This section sets out the general contract provisions that should be included in contracts.

1. The contract must incorporate the Act's definitions of "personal information" and "record".

2. The contract must state that the public body is only transferring *physical custody* of personal information to the contractor, not *control* of that information, and must state that authority over personal information use, disclosure, access, destruction and integrity remains with the public body. The contract should state how the public body can exercise that control (*e.g.*, by giving a notice to the contractor that requires the contractor to do what is specified in the notice).

3. The contractor must be required to comply with the fair information practices in Part 3 of the Act and to implement appropriate security measures required under the contract.

4. The contractor must be required to appoint a knowledgeable senior person within its organization to be responsible for privacy compliance and to be the contact for such issues. That person must have the necessary authority to do these things. The public body must be required to do the same.

5. The public body should carefully consider whether the contractor should be allowed to sub-contract any services under the contract. If sub-contracting is allowed, only qualified sub-contractors should be permitted. The contractor should be required to ensure that any sub-contract requires the sub-contractor to comply with the privacy provisions of the contract between the contractor and the public body. The public body should consider requiring the contractor to get the public body's express, written approval of sub-contract provisions before the sub-contract is signed, with the public body having the discretion to refuse approval if it reasonably considers the proposed sub-contractor does not have the experience and capacity to perform the sub-contract.

6. If the contract allows the contractor or any subcontractor to have access to personal information, the contract must expressly specify how, why and when access is permitted.

3.2 Personal Information Storage and Access – The contract should contain the following provisions dealing with the storage of, and access to, personal information.

1. The contractor should be required to:

   (a) take a physical inventory, at least annually, of all records containing personal information, to identify any losses;

(b) ensure that records are not removed from storage premises without appropriate written authorization;

(c) use physically secure areas for the storage of records and restrict access to authorized personnel;

(d) ensure that access to documentation about computer systems that contain personal information is restricted to authorized personnel;

(e) ensure that users of a system or network that processes personal information are uniquely identified and that, before a user is given access to the system or personal information, their identification is authenticated each time;

(f) implement procedures for *identification* and *authentication*, which include:

(i) controls for the issue, change, cancellation and audit-processing of user identifiers and authentication mechanisms;

(ii) ensuring that authentication codes or passwords:

(A) are generated, controlled and distributed so as to maintain the confidentiality and availability of the authentication code;

(B) are known only to the authorized user of the account;

(C) are pseudo-random in nature or vetted through a verification technique designed to counter triviality and repetition;

(D) are no fewer than 6 characters in length;

(E) are one-way encrypted;

(F) are excluded from unprotected automatic log-on processes; and

(G) are changed at irregular and frequent intervals at least semi-annually;

(g) maintain and implement formal procedures for terminated employees who have access to personal information, with prompts to ensure revocation or retrieval of identity badges, keys, passwords and access rights;

(h) position system display units and hardcopy documents, or equip them with protective material, so that any personal information being displayed or processed cannot be viewed by unauthorized persons;

(i) implement automated or manual controls to prevent unauthorized copying, transmission or printing of personal information;

(j) design and implement a public body-approved automated, always-on auditing system, that is available to the public body for monitoring access to and the use of personal information in the custody of, or managed by, the contractor;

(k) ensure that, bearing in mind the OIPC's *Guidelines for Audits of Automated Personal Information* OIPC Guideline 01-01 http://www.oipc.bc.ca/publications/advice/audit-3.pdf, the audit system referred to in 1(j) creates audit trails that automatically:

(i) record the identity of anyone who accesses, views, alters, deletes or uses a record containing personal information for any purpose, or attempts to do any of those things, and records the date and time of any such actions; and
(ii) flag accesses, or access attempts, that fall outside of set criteria (*e.g.*, access outside regular working hours); and

(l) implement control procedures to ensure the integrity of the personal information being stored, notably its accuracy and completeness.

2. The contractor must store personal information on agreed-upon media in accordance with prescribed techniques that store the personal information in a form that only authorized persons may access. These techniques may include translating the personal information into code (*encryption*) or shrinking or tightly packaging the personal information into unreadable form (*compression*).

3. The contract should specify the location where personal information will be stored.

4. The contractor must ensure that it stores backup copies of records off-site under conditions which are the same as or better than originals.

5. The contractor should be required to securely segregate personal information from information owned by others (including the contractor), including by installing *access barriers* to prevent information elements from being associated (including compared or linked, based on similar characteristics) with other information, including:

(i) separate storage facilities for the public body's personal information;
(ii) authorization before a person is granted access to computers containing such personal information; and

(iii) entry passwords and the employment of public key encryption/smart card technology where practicable.

6. The contractor must be required to ensure the integrity of personal information stored, processed or transmitted through its system or network.

7. The contractor should be required to take all reasonable steps to ensure personal information is accurately recorded, complete, updated and not deleted or altered except as directed by the public body in writing.

8. The contract should establish a process by which individuals can access their own personal information, in the custody of the contractor, through an access request under, and as permitted by, the Act.

9. The contract should require the contractor to co-operate with, and assist in, any public body investigation of a complaint that personal information has been used or disclosed contrary to the Act or the contract.

10. The contract should give the public body a right of access to the contractor's premises to recover any or all of its records and for auditing purposes to ensure contract compliance.

3.3 Enforcing Privacy and Security – It is crucial that the public body have meaningful, practical methods to monitor and enforce compliance.

1. There should be significant, effective remedies and penalties for violation of contract terms and conditions governing personal information. This should include processes for dispute resolution, and for determining appropriate remedies, if contractors or sub-contractors breach the contract.

2. The contract should require the contractor to ensure that employees engaged in performance of the contract, and any sub-contract, sign a privacy and confidentiality agreement which includes a clause specifying that discipline, up to and including termination of employment, may result if an employee, without authority, accesses, uses, discloses or disposes of personal information contrary to the contract. The contractor should be required to regularly refresh this agreement with employees.

3. The contractor should assume full responsibility for any negligent or wilful act or omission of any of its employees or sub-contractors respecting unauthorized access, use or disclosure of personal information. The contractor should be required to indemnify the public body for any liability the public body incurs as a result of unauthorized access, use or disclosure.

4. The contractor should be required to comply with the public body's retention, destruction and archival storage of personal information. At the very least, the contract should stipulate that the contractor must not destroy personal information unless the public body has identified the relevant personal information in writing and expressly directed its destruction.

5. The contractor should be required to return personal information to the public body, or destroy it, on termination of the agreement.

6. The contractor must receive personal information from the public body and disclose it only to the appropriate public body, or to agents authorized expressly in writing by the public body that provided the personal information, and then only through approved processes.

3.4 Encouraging Good Privacy Practices – Ongoing education and training are key to proper privacy protection. The contract should therefore include provisions addressing the following points.

1. At the start of the contract's term, and periodically during the term, the public body should provide appropriate guidance on the Act and its requirements to the contractor and its employees.

2. The contractor should be required to provide appropriate and ongoing training on the Act and the contract, and their requirements, to its employees and, where practicable, to approved sub-contractors and their employees. The contractor should, at a minimum, be required to include in any sub-contract provisions that implement paras. 3.3.1 through 3.3.3, above (and such other of these guidelines as are applicable).

3.5 Other Restrictions – The contract should also deal with the following added matters.

1. The contract should prohibit the contractor from sharing, matching or mining (or otherwise combining or manipulating personal information) except as agreed-to in writing, in advance, by the public body and subject always to what is permitted under the Act. Any current or new activities of these kinds that are agreed to by the parties must be subject to a new PIA undertaken by the contractor or sub-contractor in consultation with the public body.

2. The contract should prohibit the contractor from withholding personal information to enforce payment by the public body or in any contract dispute.